

MDS iNET Series

MDS iNET-II 900™

MDS iNET 900™



Wireless IP/Ethernet Transceiver

iNET-II 900 and iNET 900 Firmware Release 8.1.1 and later

MDS 05-2806A01, Rev. L

OCTOBER 2014



Digital Energy
MDS

Quick-Start instructions for this product are contained in publication 05-2873A01.

Visit our web site for downloadable copies of all documentation at **www.gemds.com**.

TABLE OF CONTENTS

1.0 Product Overview and Applications..... 1

1.1 About This Manual..... 1

1.1.1 Related Publication 1

1.2 Product Description..... 1

1.2.1 Rugged Packaging 1

Simple Installation..... 1

Secure Operation..... 2

Robust Radio Operation 2

Flexible Services..... 2

Flexible Management..... 2

Transceiver Features 2

1.2.2 Model Offerings 3

1.2.3 Differences Between iNET and iNET-II Models 3

1.2.4 MDS P21 Protected Network (Redundant) Configuration 4

1.3 Applications..... 4

1.3.1 Wireless LAN 4

1.3.2 Point-to-Point LAN Extension 5

1.3.3 Backhaul for Serial Radio Networks 5

1.3.4 Multiple Protocols and/or Services 6

1.3.5 Wireless LAN with Mixed Services 7

1.3.6 Upgrading Older Wireless Networks with Serial Interfaces 7

Replacing Legacy Wireless Products 7

Supplement Legacy Wireless Networks with IP Services..... 8

1.3.7 High-Speed Mobile Data 8

1.4 Network Design Considerations..... 8

1.4.1 Extending Network Coverage with Repeaters 8

What is a Repeater System? 8

Option 1—Using Two Transceivers to Form a Repeater Station (back-to-back repeater) 8

Option 2—Using the AP as a Store-and-Forward Packet Repeater 9

1.4.2 Protected Network Operation using Multiple Access Points 9

1.4.3 Collocating Multiple Radio Networks 10

The Network Name and the association process 10

Can radio frequency interference (RFI) disrupt my wireless network? 10

1.5 Cyber Security 11

1.6 Accessories..... 12

2.0 Embedded Management System 14

2.1 Introduction 14

2.1.1 Differences in the User Interfaces 16

2.2 Accessing the Menu System..... 17

2.2.1 Methods of Control 17

2.2.2 PC Connection & Log In Procedures 17

Starting a Local Console Session (Recommended for first-time log-in)..... 17

Starting a Telnet Session 19

Starting a Web Browser Session 20

2.2.3 Navigating the Menus 21

Via Terminal Telnet or SSH Sessions

Recommended for first-time log-in 21

Logging Out Via Terminal Emulator or Telnet 21

Navigating via Web Browser 22

Logging Out Via Web Browser 22

2.3 Basic Device Information 22

2.3.1 Starting Information Screen 22

2.3.2 Main Menu 24

2.3.3 Configuring Basic Device Parameters 25

Device Information 25

Device Names Menu..... 26

Login Status Menu 27

2.4 Configuring Network Parameters..... 27

2.4.1 Network Configuration Menu 27

2.4.2 Network Interface Configuration Menu 29

Virtual LAN in iNET Series 30

Configuring for Operation with VLAN..... 30

Configuring the IP Address when VLAN Status is Enabled 31

Configuring the IP Address When VLAN Status is Disabled..... 32

2.4.3 Ethernet Port Configuration Menu 33

2.4.4 DHCP Server Configuration 35

2.4.5 SNMP Agent Configuration 36

2.4.6 Trap Manager Submenu 37

2.4.7 SNMP V3 Accounts Submenu 38

2.4.8 Prioritized AP Configuration Submenu 38

2.4.9 Bridge Configuration Submenu 39

2.5 Radio Configuration 40

2.5.1 Radio Configuration Menu 40

2.5.2 Channel Config Menu 42

2.5.3 Advanced Configuration Menu 44

2.5.4 Skip Zones Menu 44

2.5.5 Auto Data Rate Configuration Menu 45

2.5.6	Mobility Configuration Menu	47
	Additional Considerations for Mobile Operation.....	48
	At Every Mobile (Remote) Radio	48
	At Every AP Radio	48
2.6	Configuring the Serial Ports.....	49
2.6.1	Overview	49
	Com1 Port–Dual Purpose Capability	49
	TCP vs. UDP.....	49
	Serial Encapsulation	49
	TCP Client vs. TCP Server	49
	UDP Multicast	50
	PPP	50
	DF1/EIP	50
	MODBUS/TCP	50
	Data Buffering	51
	Implementing Configuration Changes.....	51
	Serial Configuration Wizard	51
2.6.2	Serial Data Port Configuration Menu	51
2.6.3	Configuring for UDP Mode	52
2.6.4	Configuring for TCP Mode	54
2.6.5	Configuring for PPP Mode	56
2.6.6	Configuring for DF1/EIP	57
2.6.7	Configuring for MODBUS/TCP Server	58
2.6.8	IP-to-Serial Application Example	58
2.6.9	Point-to-Multipoint IP-to-Serial Application Example	59
2.6.10	Point-to-Point Serial-to-Serial Application Example	61
2.6.11	Combined Serial and IP Application Example	62
	Operation and Data Flow.....	62
2.6.12	Virtual LAN in iNET-II and iNET	64
2.7	Cyber Security Configuration.....	64
2.7.1	Device Security	64
2.7.2	Wireless Security	65
	Local Authentication—Approved Remotes/Access Points List Submenu.....	66
2.7.3	RADIUS Configuration	67
	Operation of Device Authentication	67
	Operation of User Authentication.....	67
2.7.4	RADIUS Configuration	68
2.7.5	Certificate Management (Remote transceivers only)	68
2.8	Performance Verification.....	69
2.8.1	RSSI by Zone Menu (Remotes Only)	71
2.8.2	Event Log Menu	71
	Time and Date.....	72
	View Current Alarms	73
	View Event Log	73
2.8.3	Packet Statistics Menu	74

Wireless Packet Statistics	74
Ethernet Packet Statistics	74
Packets Received by Zone	75
2.8.4 Wireless Network Status (Remotes Only)	76
The Transceiver's Association Process	76
2.8.5 Remote Listing Menu (Access Points Only)	78
2.8.6 Endpoint Listing Menu (Access Points Only)	79
2.8.7 Remote Performance Listing Menu (Access Points Only)	80
2.8.8 Bridge Status Menu	81
2.8.9 Serial Data Statistics Menu	81
2.9 Maintenance	82
2.9.1 Reprogramming Menu	83
Upgrading the Firmware	84
Error Messages During File Transfers	86
2.9.2 Configuration Scripts Menu	87
How Configuration Files Work	87
Editing Configuration Files	88
2.9.3 Authorization Key Menu	89
2.9.4 Change the Type of Remote	89
2.9.5 Auto-Upgrade/Remote-Reboot Menu	90
Firmware Upgrade (with AP Acting as a TFTP Server)	90
2.9.6 Radio Test Menu	90
2.9.7 Ping Utility Menu	92
2.9.8 Reset to Factory Defaults	92
Password Reset to Factory Default	92
2.9.9 Support Bundle	92
3.0 Troubleshooting.....	94
3.1 Introduction.....	94
3.1.1 Multiple Communication Layers	94
3.1.2 Unit Configuration	94
3.1.3 Factory Assistance	94
3.2 Troubleshooting with LEDs	95
3.3 Troubleshooting with the Menu System.....	95
3.3.1 Starting Information Screen	97
3.3.2 Packet Statistics Menu	98
3.3.3 Serial Port Statistics Menu	98
3.3.4 Diagnostic Tools	98
3.4 Using Logged Operation Events	99
3.5 Alarm/Event Conditions	99
3.6 Correcting Alarm Conditions	100

3.7	Logged Events	102
-----	---------------------	-----

4.0 Planning a Radio Network 106

4.1	Installation Planning.....	106
-----	----------------------------	-----

4.1.1	General Requirements	106
	Unit Dimensions.....	107
	DIN Rail Mounting Option	108
4.1.2	Site Selection	108
4.1.3	Equipment Grounding—Important	109
4.1.4	Terrain and Signal Strength	109
4.1.5	Antenna & Feedline Selection	109
	Antennas.....	109
	Feedlines	110
4.1.6	How Much Output Power Can be Used?	112
4.1.7	Conducting a Site Survey	112
4.1.8	A Word About Radio Interference	112
	Calculating System Gain.....	113
4.1.9	Notes on Using 28 VDC Power Supplies	113
4.2	Radio (RF) Measurements.....	114

4.2.1	Antenna System SWR and Transmitter Power Output	114
	Introduction	114
	Procedure	115
4.2.2	Antenna Aiming	115
	Introduction	115
	Procedure	115
4.3	dBm-Watts-Volts Conversion Chart	117

4.4	Performance Notes	117
-----	-------------------------	-----

4.4.1	Wireless Bridge	117
4.4.2	Distance-Throughput Relationship	118
4.4.3	Data Latency—TCP versus UDP Mode	118
4.4.4	Data Compression	118
4.4.5	Packets-per-Second (PPS)	118
4.4.6	Station-to-Station Traffic	119
4.4.7	Interference has a Direct Correlation to Throughput	119
4.4.8	Maximizing Throughput	119
4.4.9	Placing an iNET Radio Behind a Firewall	120

4.5	SNMPv3 Notes	120
-----	--------------------	-----

4.5.1	Overview	120
	SNMPv3 Accounts	120
	Context Names	121
	Password-Mode Management Changes.....	121

5.0 Technical Reference 124

5.1 Data Interface Connectors 124

5.1.1 LAN Port 124

5.1.2 COM1 Port 125

5.1.3 COM2 Port 125

5.2 Fuse Replacement..... 126

5.3 Technical Specifications..... 126

5.4 Channel Hop Table 129

APPENDIX A—MDS iNET/ENI Protocols..... 132

APPENDIX B—Glossary of Terms & Abbreviations..... 148

Copyright and Publication Notices

This publication is protected under copyright law. Copyright 2014, GE MDS. All rights reserved.

Historical revision note: There was no “Rev. I” issued for this manual, to avoid confusion with the digit “1.” Publication went from Rev. H directly to Rev. K.

ISO 9001 Registration

GE MDS adheres to this internationally-accepted ISO 9001 quality system standard.

To our Customers

We appreciate your patronage. You are our business. We promise to serve and anticipate your needs. We will strive to give you solutions that are cost effective, innovative, reliable and of the highest quality possible. We promise to build a relationship that is forthright and ethical, one that builds confidence and trust.

Products Covered in this Manual

This manual covers two members of the MDS iNET Transceiver Series, both of which are designed to be operated under the FCC’s Part 15 license-free rules. The iNET radio is a Frequency Hopping Spread Spectrum (FHSS) transceiver that operates at data speeds of 256 and 512 kbps.

The iNET-II is a similar design, but it is certified under the Digital Transmission System (DTS) provisions of FCC Part 15 and can operate at data speeds of 512 or 1024 kbps. Operational differences between these two models are identified, where necessary, in this manual.

NOTE: MDS iNET and MDS iNET-II transceivers are *not* over-the-air compatible.

Other MDS iNET 900 Series Documentation

Quick Start Guide—The MDS iNET 900 Series Quick Start Guide, P/N 05-2873A01, is provided with the transceiver and is limited to essential information needed for installers. The installation guide assumes some guidance to installers will be provided by the readers of this manual. This includes such things as antenna selection, radio communication site survey tools and techniques, and network design.

Related Materials on the Internet—Data sheets, frequently asked questions, case studies, application notes, firmware upgrades and other updated information is available on the GE MDS Web site at www.gemds.com.

About GE MDS

Almost two decades ago, GE MDS began building radios for business-critical applications. Since then, we've installed over a million radios in over 110 countries. To succeed, we overcame impassable terrain, brutal operating conditions and disparate, complex network configurations. We also became experts in wireless communication standards and system applications worldwide. The result of our efforts is that today, thousands of utilities around the world rely on GE MDS-based wireless networks to manage their critical assets.

The majority of our radios deployed since 1985 are still installed and performing within our customers' wireless networks. That's because we design and manufacture our products in-house, according to ISO 9001 which allows us to control and meet stringent global quality standards.

Thanks to our durable products and comprehensive solutions, GE MDS is the wireless leader in industrial automation—including oil and gas production and transportation, water/wastewater treatment, supply and transportation, electric transmission and distribution and many other utility applications. GE MDS is also at the forefront of wireless communications for private and public infrastructure and online transaction processing. Now is an exciting time for GE MDS and our customers as we look forward to further demonstrating our abilities in new and emerging markets.

As your wireless needs change you can continue to expect more from us. We'll always put the performance of your network above all. Visit us at www.gemds.com for more information.

Product Test Data Sheets

Test Data Sheets showing the original factory test results for this unit are available upon request from the GE MDS Quality Leader. Contact the factory using the information at the back of this manual. Serial numbers must be provided for each product where a Test Data Sheet is required.

OPERATIONAL & SAFETY NOTICES

RF Exposure



Professional installation required. The radio equipment described in this guide emits radio frequency energy. Although the power level is low, the concentrated energy from a directional antenna may pose a health hazard. Do not allow people to come closer than 23 cm (9 inches) to the antenna when the transmitter is operating in indoor or outdoor environments. More information on RF exposure is on the Internet at www.fcc.gov/oet/info/documents/bulletins.

UL/CSA Notice

This product is available for use in Class 1, Division 2, Groups A, B, C & D Hazardous Locations. Such locations are defined in Article 500 of the National Fire Protection Association (NFPA) publication NFPA 70, otherwise known as the National Electrical Code.

The transceiver has been recognized for use in these hazardous locations by two independent agencies —Underwriters Laboratories (UL) and the Canadian Standards Association (CSA). The UL certification for the transceiver is as a Recognized Component for use in these hazardous locations, in accordance with UL Standard 1604. The CSA Certification is in accordance with CSA STD C22.2 No. 213-M1987.

UL/CSA Conditions of Approval: The transceiver is not acceptable as a stand-alone unit for use in the hazardous locations described above. It must either be mounted within another piece of equipment which is certified for hazardous locations, or installed within guidelines, or conditions of approval, as set forth by the approving agencies. These conditions of approval are as follows:

The transceiver must be mounted within a separate enclosure which is suitable for the intended application.

The antenna feedline, DC power cable and interface cable must be routed through conduit in accordance with the National Electrical Code.

Installation, operation and maintenance of the transceiver should be in accordance with the transceiver's installation manual, and the National Electrical Code.

Tampering or replacement with non-factory components may adversely affect the safe use of the transceiver in hazardous locations, and may void the approval.

A power connector with screw-type retaining screws as supplied by GE MDS must be used.



Do not disconnect equipment unless power has been switched off or the area is known to be non-hazardous.

Refer to Articles 500 through 502 of the National Electrical Code (NFPA 70) for further information on hazardous locations and approved Division 2 wiring methods.

FCC Part 15 Notices

The transceiver series complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This device is specifically designed to be used under Section 15.247 of the FCC Rules and Regulations. Any unauthorized modification or changes to this device without the express approval of Microwave Data Systems may void the user's authority to operate this device. Furthermore, the iNET Series is intended to be used only when installed in accordance with the instructions outlined in this manual. Failure to comply with these instructions may also void the user's authority to operate this device.

Part 15 rules also require that the Effective Isotropic Radiated Power (EIRP) from an GE MDS iNET Series installation not exceed 36 dBm. Refer to [Antenna & Feedline Selection on Page 108](#) for more information.

Industry Canada RSS Notices

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

To reduce potential radio interference to other users, the antenna type and its gain should be chosen so that the Equivalent Isotropic Radiated Power (EIRP) is not more than that permitted for successful communication.

This device has been designed to operate with the antennas listed below, and having a maximum gain of 12 dB. Antennas not included in this list or having a gain greater than 12 dB are strictly prohibited for use with this device. The required antenna impedance is 50 ohms. The *Antenna & Feedline Selection on Page 108* discusses antennas acceptable for use with this transceiver.

Manual Revision and Accuracy

This manual was prepared to cover a specific version of firmware code. Accordingly, some screens and features may differ from the actual unit you are working with. While every reasonable effort has been made to ensure the accuracy of this publication, product improvements may also result in minor differences between the manual and the product shipped to you. If you have additional questions or need an exact specification for a product, please contact our Customer Service Team using the information at the back of this guide. In addition, manual updates can often be found on the GE MDS Web site at www.gemds.com.

Environmental Information



The manufacture of this equipment has required the extraction and use of natural resources. Improper disposal may contaminate the environment and present a health risk due to hazardous substances contained within. To avoid dissemination of these substances into our environment, and to limit the demand on natural resources, we encourage you to use the appropriate recycling systems for disposal. These systems will reuse or recycle most of the materials found in this equipment in a sound way. Please contact GE MDS or your supplier for more information on the proper disposal of this equipment.

Battery Disposal

This product may contain a battery. Batteries must be disposed of properly, and may not be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. Batteries are marked with a symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling return the battery to your supplier or to a designated collection point.

1.0 PRODUCT OVERVIEW AND APPLICATIONS

1.1 About This Manual

This Reference Manual is designed for use by professional installers and technicians. It contains an in-depth description of the product, including installation, configuration, and troubleshooting details.

1.1.1 Related Publication

A companion publication, the *iNET Series Start-Up Guide* is also available (Part No. 05-2873A01). This smaller guide contains the essential information for installing the radio and placing it into operation. This guide is recommended for those primarily involved in the installation and setup of the product.

1.2 Product Description

The GE MDS iNET 900 transceiver (Figure 1-1) provides an easy-to-install wireless local area network (WLAN) service with long range and secure operation. It supports both Ethernet *and* serial data interface options at over-the-air data speeds of up to 1 Mbps (iNET-II) and 512 kbps (iNET).

NOTE: For information on the MDS iNET 900 ENI, which provides expanded gateway and protocol conversion capabilities not found in the iNET 900 (DF1 to EIP, and MODBUS to MODBUS TCP conversions), refer to Appendix A, *MDS iNET/ENI Protocols* (beginning on Page 132).



Figure 1-1. The GE MDS iNET 900 Transceiver

1.2.1 Rugged Packaging

The transceiver is housed in a compact and rugged cast-metal case that need only be protected from direct exposure to the weather. It contains a single printed circuit board with all necessary components for radio operation and data communications. The only user-serviceable component in the case is a fuse on the DC power input line.

Simple Installation

Most installations employ an omni-directional antenna at the Access Point (AP) location and a directional antenna at each Remote unit. The antenna is a vital link in the system and must be chosen and installed correctly. See “Installation Planning” on Page 106 for guidance on choosing suitable installation sites and antennas.

For basic services, simply connect an antenna, connect your Ethernet LAN to the transceiver's LAN port, apply primary power, set a few operating parameters, and you are done. No license is required for operation in the U.S.A., Canada, and many other countries. Check requirements for your region before placing the transceiver in service.

Secure Operation

Data network security is a vital issue in today's wireless world. MDS iNET Series radios provide multiple tools to help you build a network that minimizes the risk of eavesdropping and unauthorized access. Some are inherent in the radio's operation, such as the use of 900 MHz spread-spectrum transmissions; others include data encryption, enabling/disabling remote access channels, and password protection.

Remember, security is not a one-step process that can simply be turned on and forgotten. It must be practiced and enforced at multiple levels, 24 hours-a-day and 7 days-a-week. See "Cyber Security" on Page 11 for more information about the transceiver's security tools.

Robust Radio Operation

The transceiver is designed for frequency-hopping spread-spectrum operation in the license-free 900 MHz Industrial, Scientific, and Medical (ISM) band. It can provide reliable communications at distances up to 25 miles (40 km) over favorable terrain, even in the presence of weak signals or interference. Frequency hopping allows the transceiver to avoid interference from other transmitters in the same band, and provides frequency diversity for more reliable transmission. The over-the-air MAC increases reliability by adding retries to failed messages.

The iNET-II transceiver, which is certified to operate under DTS rules (hopping not required), also hops in order to achieve the same benefits that are realized with the iNET transceiver which is certified under FHSS rules.

Flexible Services

Users with a mixture of equipment having Ethernet and serial data interfaces can choose to use one or two of the user-configurable serial ports through the use of a Remote Dual Gateway. This flexibility allows the transceiver to provide services in data networks that are being migrated from legacy serial/EIA-232-based hardware to the faster and more easily interfaced Ethernet world.

Flexible Management

Configuration, commissioning, troubleshooting and other maintenance activities can be done locally or remotely. Four different modes of access are available: local RS-232 console, local or remote Internet Protocol (IP) access via Telnet or SSH, web browser (HTTP, HTTPS), and SNMP (v1/v2/v3). The text-based interface (RS-232 console Telnet and SSH) is implemented in the form of easy-to-follow menus, and the terminal server configuration includes a wizard to help you set up the units correctly.

Transceiver Features

The transceiver's design makes the installation and configuration easy, while allowing for changes in the future.

- Long Range operation in line-of-sight conditions. Repeater stations may be used to extend the range. (Refer to "TRANSMIT/RECEIVE RANGE (Nominal)" on Page 129 for more detailed information on range.)
- Industrial-Grade Product—Extended temperature range for trouble-free operation in extreme environments
- Robust Radio Communications—Designed to operate in dense, high-interference environments
- Robust Network Security—Prevents common attack schemes and hardware from gaining access or control of network. Common attack events logged and reported by alarms.
- High Speed—1 Mbps (iNET-II) is 100-times faster than 9.6 kbps radios. MDS iNET transceiver speed is 512 kbps.
- Plug-and-Play Connectivity—Ethernet bridge configuration option requires minimal setup

- Serial Ports—Gateway for serial-based equipment to IP/Ethernet networks with embedded terminal server. Site-to-site configurations are also possible.
- Single hardware package provides configuration as Access Point or Remote

1.2.2 Model Offerings

The transceiver comes in two primary models—**Access Point** and **Remote**. Additionally, three types of Remote Gateways are available—the *Ethernet Bridge*, the *Serial Gateway*, and the *Dual Gateway* supporting both IP/Ethernet and serial services. Table 1-1 summarizes the different interface abilities for each type.

A unit can be configured by the owner to operate as an Access Point or as a Remote with some restrictions. Only the Dual Gateway Remote units can be reconfigured as an Access Point. Ethernet Bridge and Serial Gateway Remotes cannot be reconfigured as an Access Point unless they are first upgraded to Dual Gateway type. This is accomplished with an “Authorization Key” purchased from the factory. Each one of these individual software keys is associated with the serial number of the corresponding unit.

Table 1-1. Transceiver Models and Data Interface Services

Model	Type	LAN ¹	COM1 ¹	COM2
Access Point ²	N/A	Yes	Yes	Yes
Remote...	Ethernet Bridge ³	Yes	No	No
	Serial Gateway ³	No	Yes	Yes
	Dual Gateway ²	Yes	Yes	Yes

NOTES

1. Provides access to the embedded Management System on all units.
2. Can be configured as an Access Point or Dual Gateway through the embedded Management System.
3. Can be upgraded to Dual Gateway with an Authorization Key.

1.2.3 Differences Between iNET and iNET-II Models

The iNET and iNET-II Transceivers, while similar in many respects, do have some important differences. The main differences are summarized in Table 1-2:

Table 1-2. Transceiver Differences (iNET vs. iNET-II)

Characteristic	iNET	iNET-II
Data Rate	256/512 kbps	512 kbps/1 Mbps
FCC Certification Type	FHSS	DTS
Encryption	RC4-128	AES-128
Channel size	316.5 kHz	600 kHz
Channel operation	Zones	Channels
Firmware	Specific for iNET	Specific for iNET-II

NOTE: The MDS iNET and MDS iNET-II transceivers are *not* over-the-air compatible.

NOTE: The radio does not support the simultaneous use of Fragmentation and Encryption. If encryption is enabled (other than RADIUS), the fragmentation option will not be available.

1.2.4 MDS P21 Protected Network (Redundant) Configuration

For mission-critical applications, GE MDS also offers the Protected Network Station. This radio incorporates two iNET Series transceivers, two power supplies, and a switchover logic board that automatically selects between Transceiver A and Transceiver B as the active radio. Figure 1-2 shows a view of the protected chassis. For system-level information on this product, see publication 05-4161A01.

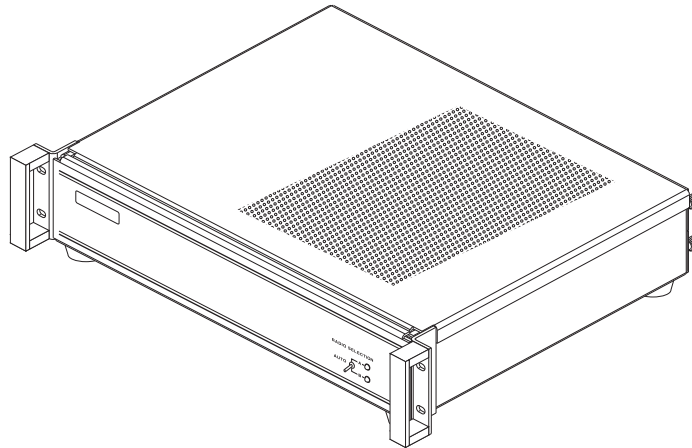


Figure 1-2. MDS P21 Protected Network Station
(Incorporates Two Transceivers, with Automatic Switchover)

1.3 Applications

The following sections provide illustrations of typical transceiver installations. This is meant as an overview only. It is recommended that a network manager be involved in all installation planning activities.

1.3.1 Wireless LAN

The wireless LAN is the most common application of the transceiver. It consists of a central control station (Access Point) and one or more associated Remote units, as shown in Figure 1-3 on Page 5. A LAN provides communications between a central WAN/LAN and remote Ethernet segments. The operation of the radio system is transparent to the computer equipment connected to the transceiver.

The Access Point is positioned at a location from which it can communicate with all of the Remote units in the system. Commonly, this is a high location on top of a building or communications tower. Messages are exchanged at the Ethernet level. This includes all types of IP traffic.

A Remote transceiver can only talk over-the-air to an Access Point unit (AP). Peer-to-peer communications between Remotes can only take place indirectly via the AP. In the same fashion, an AP can only talk over-the-air to associated Remote units. Exception: Two APs can communicate with each other “off-the-air” through their Ethernet connectors using a common LAN/WAN.

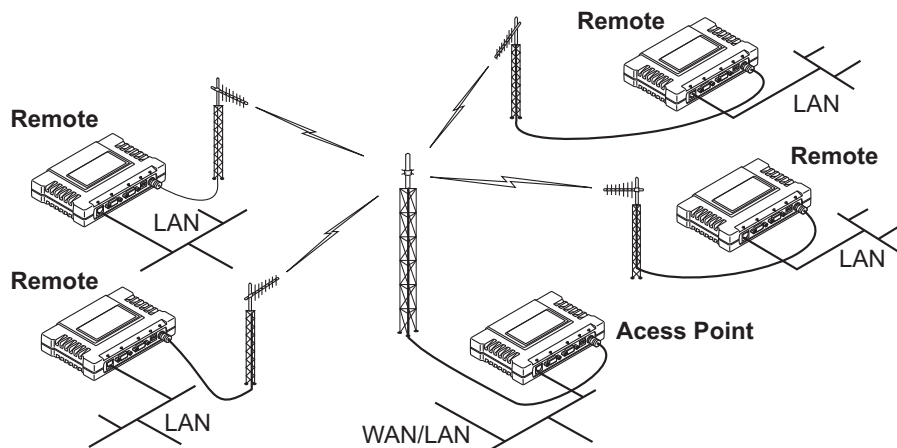


Figure 1-3. Typical Wireless LAN

1.3.2 Point-to-Point LAN Extension

A point-to-point configuration (Figure 1-4) is a simple arrangement consisting of an Access Point and a Remote unit. This provides a communications link for the transfer of data between two locations.

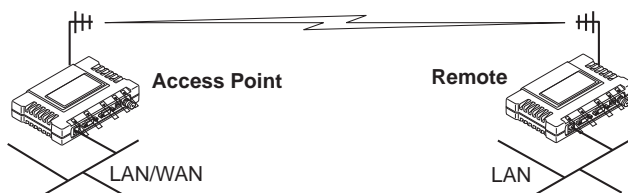


Figure 1-4. Typical Point-to-Point Link

1.3.3 Backhaul for Serial Radio Networks

One of the primary design features of the transceiver is to provide a path for serial devices to migrate to IP/Ethernet. Many radio networks in operation today still rely on serial networks at data rates of 9600 bps or less. These networks can use the transceiver as a means to continue using the serial service, while allowing the rest of the infrastructure to migrate to an IP format.

A Remote transceiver using one serial port for the data stream, and the other for network-wide diagnostics can support operational radio networks built with serial-based radios, such as MDS x790/x710, MDS TransNET and others. In the case of radios using a single port for data and diagnostics, the capabilities are doubled. The data streams are delivered to an IP socket in an application, or in serial format using the Access Point. See Figure 1-5 on Page 6.

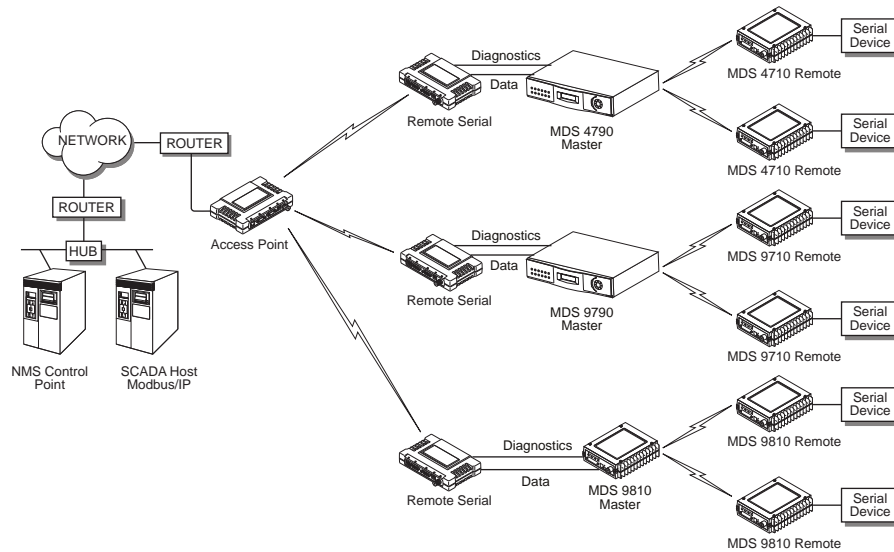


Figure 1-5. Backhaul Network

1.3.4 Multiple Protocols and/or Services

Prior to the iNET Series, two radios were often used to service two different types of devices (typically connected to different SCADA hosts). An iNET or iNET-II radio provides this functionality with a single remote radio. Each of the two serial ports can be connected via IP to different SCADA hosts, transporting different (or the same) protocols. Both data streams are completely independent and the transceiver provides seamless simultaneous operation as shown in Figure 1-6.

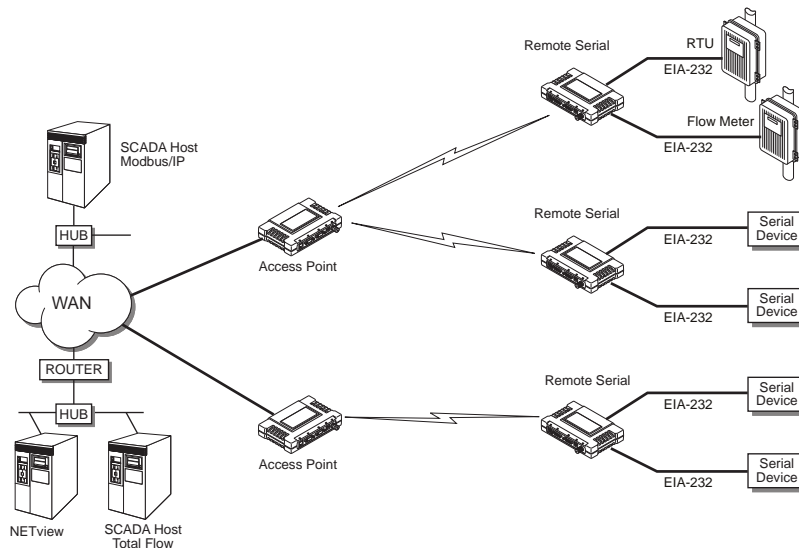


Figure 1-6. Multiple Protocol Network

By using a single radio, the cost of deployment is cut in half. Beyond requiring only one radio instead of two, the biggest cost reduction comes from using half of the required infrastructure at the remote site: one antenna, one feedline, one lightning protector and ancillary hardware. Other cost reductions come from the system as a whole, such as reduced management requirements. And above all, the radio offers potential for future applications that run over Ethernet and IP, such as video for remote surveillance.

1.3.5 Wireless LAN with Mixed Services

The iNET transceiver is an excellent solution for a long-range industrial wireless LAN. It offers several advantages over commercial solutions—primarily improved performance over extended distances. The rugged construction of the radio and its extended temperature range make it an ideal solution even in harsh locations. In extreme environments, a simple NEMA enclosure is sufficient to house the unit.

The transceiver trades higher speed for longer range. Commercial 802.11a/b/g solutions are designed to provide service to relatively small areas such as offices, warehouses and homes. They provide high data rates but have limited range. The iNET transmits at a higher power level, uses a different frequency band, has higher sensitivity, and a narrower channel to concentrate the radio energy and reach farther distances. It is designed for industrial operation from the ground up.

IP-based devices that may be used with the transceiver include a new breed of more powerful Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs). These, as well as other devices, may be used in applications ranging from SCADA/telemetry monitoring, web-based video, security monitoring, and voice over IP. Figure 1-7 shows a typical wireless IP network.

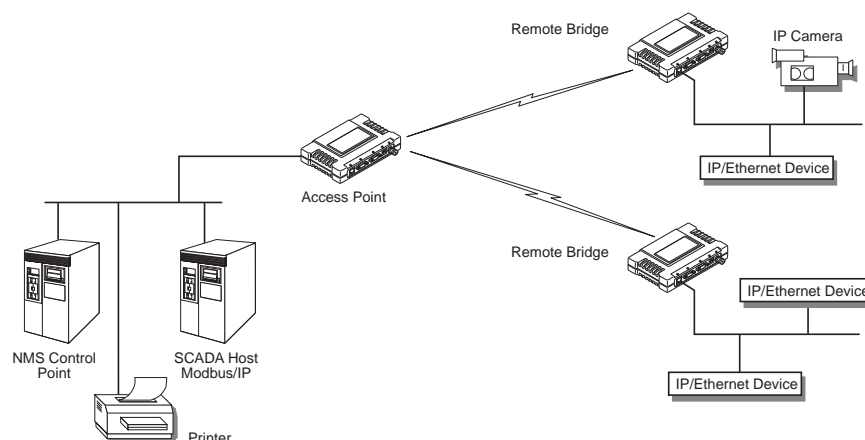


Figure 1-7. Extended-Range LAN with Mixed Applications

1.3.6 Upgrading Older Wireless Networks with Serial Interfaces

Millions of wireless data products have been sold in the last two decades for licensed and license-free operation, many of them manufactured by GE MDS. There are several ways that these systems can benefit from incorporating iNET equipment. The chief advantages are interface flexibility (serial and Ethernet in one unit), and higher data throughput. By taking advantage of its built-in serial and Ethernet interfaces, the transceiver is well suited to replace leased lines, dial-up lines, or existing MAS 900 MHz data transceivers.

Replacing Legacy Wireless Products

In most cases, legacy radio transceivers supporting serial-interface equipment can be replaced with iNET transceivers. Legacy equipment can be connected to the transceiver through the COM1 or COM2 port with a DB-25 to DB-9 cable wired for EIA-232 signaling. The COM2 port supports all standard EIA-232 signaling and acts as a data-terminal equipment device (DTE).

NOTE: Several previous MDS-brand products had non-standard signal lines on their interface connectors (to control sleep functions and alarm lines, for example). These special functions are not provided nor supported by the iNET Series. Consult equipment manuals for complete pinout information.

Supplement Legacy Wireless Networks with IP Services

The iNET Dual Gateway model can support up to two serial devices and one Ethernet connection at the same time. The serial interfaces (COM1 and COM2) operate in two different modes: Connectionless UDP and connection-oriented TCP.

In the UDP mode, the transceiver supports point-to-multipoint serial-port to serial-port connectivity. In the TCP mode, it supports point-to-point Ethernet/IP to serial port connectivity.

For further details on the transceiver's Serial Gateway interface modes, see “*Configuring the Serial Ports*” on Page 49.

1.3.7 High-Speed Mobile Data

The iNET radios support high-speed data communications in a mobile environment. Remote radios roam between different access points, providing seamless transitions and continuous coverage. For additional information on configuring a mobile network, refer to “*Mobility Configuration Menu*” on Page 47.

1.4 Network Design Considerations

1.4.1 Extending Network Coverage with Repeaters

What is a Repeater System?

A repeater works by re-transmitting data from outlying remote sites to the Access Point and vice-versa. It introduces some additional end-to-end transmission delay but provides longer-range connectivity.

In some geographical areas, obstacles can make communications difficult. These obstacles are commonly large buildings, hills, or dense foliage. These obstacles can often be overcome with a repeater station.

Option 1—Using Two Transceivers to Form a Repeater Station (back-to-back repeater)

Although the range between transceivers can be a nominal 40 km (25 miles) over favorable terrain, it is possible to extend the range considerably by connecting two units together at one site in a “back-to-back” fashion to form a repeater, as shown in Figure 1-8. This arrangement should be used whenever the objective is to utilize the maximum range between stations. In this case, using high-gain Yagi antennas at each location will provide more reliable communications than their counterparts—omnidirectional antennas.

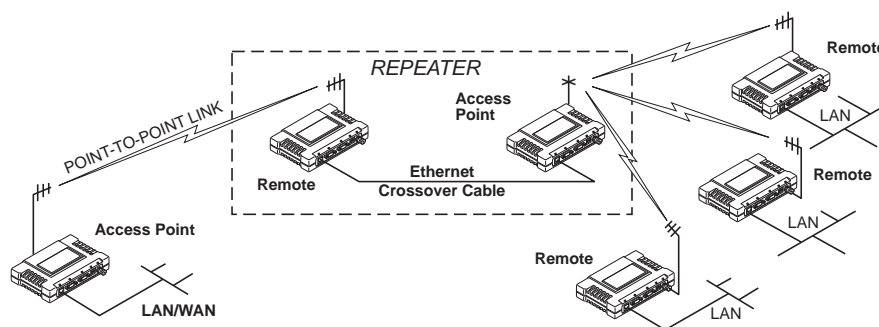


Figure 1-8. Typical LAN with a Repeater Link

Overview

Two transceivers may be connected “back-to-back” through the LAN Ports to form a repeater station. (The cable must be a “cross-over” Ethernet cable for this to work). This configuration is sometimes required in a network that includes a distant Remote that would otherwise be unable to communicate directly with the Access Point station due to distance or terrain.

The geographic location of a repeater station is especially important. A site must be chosen that allows good communication with *both* the Access Point and the outlying Remote site. This is often on top of a hill, building, or other elevated terrain from which both sites can be “seen” by the repeater station antennas. A detailed discussion on the effects of terrain is given in 4.1.2 *Site Selection*.

The following paragraphs contain specific requirements for repeater systems.

Antennas

Two antennas are required at this type of repeater station—one for each radio. Measures must be taken to minimize the chance of interference between these antennas. One effective technique for limiting interference is to employ *vertical separation*. In this arrangement, assuming both are vertically polarized, one antenna is mounted *directly* over the other, separated by at least 10 feet (3 Meters). This takes advantage of the minimal radiation exhibited by most antennas directly above and below their driven elements.

Another interference reduction technique is to cross-polarize the repeater antennas. If one antenna is mounted for polarization in the vertical plane, and the other in the horizontal plane, an additional 20 dB of attenuation can be achieved. (Remember that the corresponding stations should use the same antenna orientation when cross-polarization is used.)

Network Name

The two radios that are wired together at the repeater site *must* have different network names.

Option 2—Using the AP as a Store-and-Forward Packet Repeater

A wireless network can be extended through the use of an alternate arrangement using the Access Point as a repeater to re-transmit the signals of all stations in the network. The repeater is a standard transceiver configured as an Access Point, and operating in Store and Forward mode (see Figure 1-9).

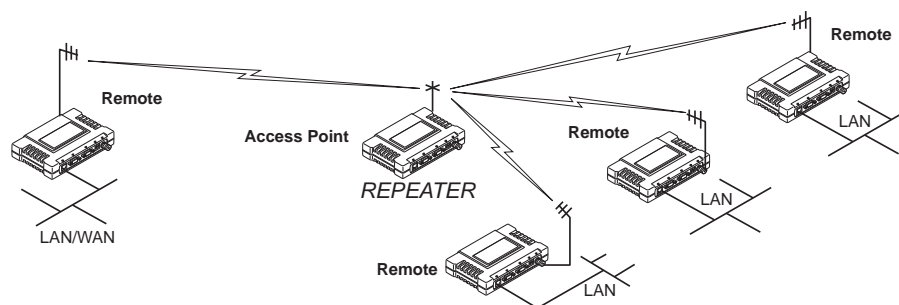


Figure 1-9. Typical network with store-and-forward repeater

As with the conventional repeater described in Option 1 above, the location of a store and forward repeater is also important. A site must be chosen that allows good communication with *both* the Access Point and the outlying Remote site. This can be on the top of a hill, building, or other elevated terrain from which all sites can be “seen” by the repeater station antenna. A detailed discussion on the effects of terrain is given in Section 4.1.2 *Site Selection*.

1.4.2 Protected Network Operation using Multiple Access Points

Although GE MDS transceivers have a very robust design and have undergone intensive testing before being shipped, it is possible for isolated failures to occur. In mission-critical applications, down time can be virtually eliminated by using some, or all, of the following configurations:

In a point-to-multipoint scenario, the Access Point services multiple remotes. A problem in the Access Point will have an effect on all remotes, since none will have access to the network. When operation of the network does not tolerate any down time, it is possible to set up a protected configuration for the Access Point to greatly reduce the possibility of this occurrence. An MDS P21 Protected Network Station may be used to achieve redundant operation. It employs two APs in a single enclosure, with appropriate switching circuits.

In this application, two or more Access Points are configured with the same Network Name and kept active simultaneously, each with its own independent antenna. In this scenario, Remotes will associate with either one of the available Access Points. In case of a failure of one of the AP's the Remotes will quickly associate with another of the remaining Access Points re-establishing connectivity to the end devices.

The Access Points are unaware of the existence of the other AP's. Because the hopping algorithm uses *both* the Network Name *and* the Wireless MAC address of the AP to generate the hopping pattern, multiple AP's can coexist—even if they use the same network name. The collocated AP's will be using different hopping patterns and frequencies the great majority of the time. Although some data collisions will occur, the wireless-MAC is built to tolerate and recover from such occurrences with minimal degradation.

1.4.3 Collocating Multiple Radio Networks

Many networks can operate in relatively close physical proximity to one another provided reasonable measures are taken to assure the radio signal of one Access Point is not directed at the antenna of the second Access Point.

The Network Name and the association process

The Network Name is the foundation for building individual radio networks. It is part of a beacon signal broadcast by the Access Point (AP) to any Remote units with the same Network Name. Remotes that join the network are referred to as being “associated” with the Access Point unit.

Multiple APs with the same Network Name should be used with care. Using the same Network Name in multiple APs may result in Remotes associating with undesired APs and preventing data exchange from occurring as planned.

The use of a different Network Name does not guarantee an interference-free system. It does however, assure that only data destined for a unique network is passed through to that network.

Co-Location for Multiple Networks

It may be desirable to co-locate Access Points at one location to take advantage of an excellent or premium location that can serve two independent networks. Each network should have a unique Network Name, and each AP unit's antenna should be provided as much vertical separation as is practical to minimize RFI.

NOTE: All transceivers are shipped with the Network Name set to “Not Programmed.” The Network Name must be programmed in order to pass data and begin normal operations.

Can radio frequency interference (RFI) disrupt my wireless network?

When multiple radio networks operate in close physical proximity to other wireless networks, individual units may not operate reliably under weak signal conditions and may be influenced by strong radio signals in adjacent bands. This radio frequency interference cannot be predicted with certainty, and can only be determined by experimentation. If you need to co-locate two units, start by using the largest possible vertical antenna separation between the two AP antennas on the same support structure. If that does not work, consult with your factory representative about other techniques for controlling radio frequency interference between the radios. (See “A Word About Radio Interference” on Page 112 for more details.)

1.5 Cyber Security

Today the operation and management of an enterprise is becoming increasingly dependent on electronic information flow. An accompanying concern becomes the cyber security of the communication infrastructure and the security of the data itself.

The transceiver is capable of dealing with many common security issues. Table 1-3 profiles security risks and how the transceiver provides a solution for minimizing vulnerability.

Table 1-3. Security Risk Management

Security Vulnerability	GE MDS Cyber Security Solution
Unauthorized access to the backbone network through a foreign remote radio	<ul style="list-style-type: none"> • 802.1X authentication • Approved Remotes List (local) Only those remotes included in the AP list will associate
“Rogue” AP, where a foreign AP takes control of some or all remote radios and thus remote devices	<ul style="list-style-type: none"> • 802.1X authentication • Approved AP List A remote will only associate to those APs included in its local authorized list of APs
Dictionary attacks, where a hacker runs a program that sequentially tries to break a password.	<ul style="list-style-type: none"> • Failed-login lockdown After 3 tries, the transceiver ignores login requests for 5 minutes. Critical event reports (traps) are generated as well.
Denial of service, where Remote radios could be reconfigured with bad parameters bringing the network down.	<ul style="list-style-type: none"> • Remote login with SSH or HTTPS • Local console login • Disabled HTTP & Telnet to allow only local management services
Airsnort and other war-driving hackers in parking lots, etc.	<ul style="list-style-type: none"> • 900 MHz operation is not interoperable with standard 802.11b wireless cards • The transceiver cannot be put in a promiscuous mode • Proprietary data framing
Eavesdropping, intercepting messages	<ul style="list-style-type: none"> • AES-128 encryption (iNET-II) • RC4-128 encryption (iNET)
Key cracking software	<ul style="list-style-type: none"> • Automatic Rotating Key algorithm
Replaying messages	<ul style="list-style-type: none"> • Automatic Rotating Key algorithm

Table 1-3. Security Risk Management

Security Vulnerability	GE MDS Cyber Security Solution
Unprotected access to configuration via SNMPv1	<ul style="list-style-type: none"> • Implement SNMPv3 secure operation
Intrusion detection	<ul style="list-style-type: none"> • Provides early warning via SNMP through critical event reports (unauthorized, logging attempts, etc.) • Unauthorized AP MAC address detected at Remote • Unauthorized Remote MAC address detected at AP • Login attempt limit exceeded (Accessed via: Telnet, HTTP, or local) • Successful login/logout (Accessed via: Telnet, HTTP, or local)

1.6 Accessories

Table 1-4 lists common accessories and spare items for the transceiver. GE MDS also offers an *Accessories Selection Guide* listing an array of additional items that may be used with the product. Contact your factory representative or visit www.gemds.com to obtain a copy of the guide.

Table 1-4. Accessories

Accessory	Description	Part No.
AC Power Adapter Kit	A small power supply module designed for continuous service. UL approved. Input: 120/220; Output: 13.8 Vdc @ 2.5 A	01-3682A02
Omni-Directional Antenna	Rugged antennas well suited for use at Access Point installations.	97-3194A17
Yagi Antenna (Directional)	Rugged antennas well suited for use at Remote installations.	97-3194A14
Surge Protectors	125-1000MHz NF-NF Flange	97-1680A01
	125-1000MHz NF-NF Bulkhead	97-1680A05
Cable AVA5-50A	7/8-in. Foam Per Foot	97-1677A174
Cable LDF4-50A	1/2-in. Foam Per Foot	97-1677A103
Cable LMR-400	Standard Outdoor Cable Per Foot	97-3675A10
Cable RJ45 CAT5	Crossover 6-ft.	97-1870A21
	Straight 6-ft.	97-1870A20
Connector Kits (up to 1 GHz)	LDF4 TNC-M with Bulkhead Mount	97-1677A171
	LMR400 TNC-M with Bulkhead Mount	97-3675A86
	LMR400 TNC-M with Flange Mount	97-3675A76
TNC Male-to-N Female Adapter	One-piece RF adaptor plug.	97-1677A161

Table 1-4. Accessories

Accessory	Description	Part No.
TNC Male-to-N Male Jumper Cable	Short length of coaxial cable used to connect the radio's TNC antenna connector to a Type N commonly used on large diameter coaxial cables.	97-1677A159 (3 ft./1m) 97-1677A160 (6 ft./1.8m)
Ethernet RJ-45 Crossover Cable (CAT5)	Cable assembly used to cross-connect the Ethernet ports of two transceivers used in a repeater configuration. (Cable length \approx 3 ft./1M)	97-1870A21
2-Pin Power Plug	Mates with power connector on transceiver. Screw terminals provided for wires, threaded locking screws to prevent accidental disconnect.	73-1194A39
Ethernet RJ-45 Straight-thru Cable (CAT5)	Cable assembly used to connect an Ethernet device to the transceiver. Both ends of the cable are wired identically. (Cable length \approx 3 ft./1M)	97-1870A20
EIA-232 Shielded Data Cable	Shielded cable terminated with a DB-25 male connector on one end, and a DB-9 female on the other end. Two lengths available (see part numbers at right).	97-3035L06 (6 ft./1.8m) 97-3035L15 (15 ft./4.6m)
EIA-232 Shielded Data Cable	Shielded cable terminated with a DB-9 male connector on one end, and a DB-9 female on the other end, 6 ft./1.8m long.	97-1971A03
Fuse	Small, board-mounted fuse used to protect against over-current conditions.	29-1784A03
Flat-Surface Mounting Brackets & Screws	Brackets: 2" x 3" plates designed to be screwed onto the bottom of the unit for surface-mounting the radio.	82-1753-A01
	Screws: 6-32/1/4" with locking adhesive. (Industry Standard MS 51957-26)	70-2620-A01
MDS P21	Redundant iNET Chassis	
MDS P60	Basic Package Model	
DIN Rail Mounting Bracket	Bracket used to mount the transceiver to standard 35 mm DIN rails commonly found in equipment cabinets and panels.	03-4125A04
COM2 Interface Adapter	DB-25(F) to DB-9(M) shielded cable assembly (6 ft./1.8 m) for connection of equipment or other EIA-232 serial devices previously connected to "legacy" units. (Consult factory for other lengths and variations.)	97-3035A06
MDS PulseNET Software	PC-based network management system for new-generation GE MDS transceivers. Allows radio control and diagnostics in a hierarchical map perspective. For more information, go to www.gedigitalenergy.com/Communications/pulsenet.htm .	Consult factory
Bandpass Filter	Antenna system filter that helps eliminate interference from nearby paging transmitters.	20-2822A02
Ethernet Surge Suppressor	Surge suppressor for protection of Ethernet port against lightning.	29-4018A01

2.0 EMBEDDED MANAGEMENT SYSTEM

2.1 Introduction

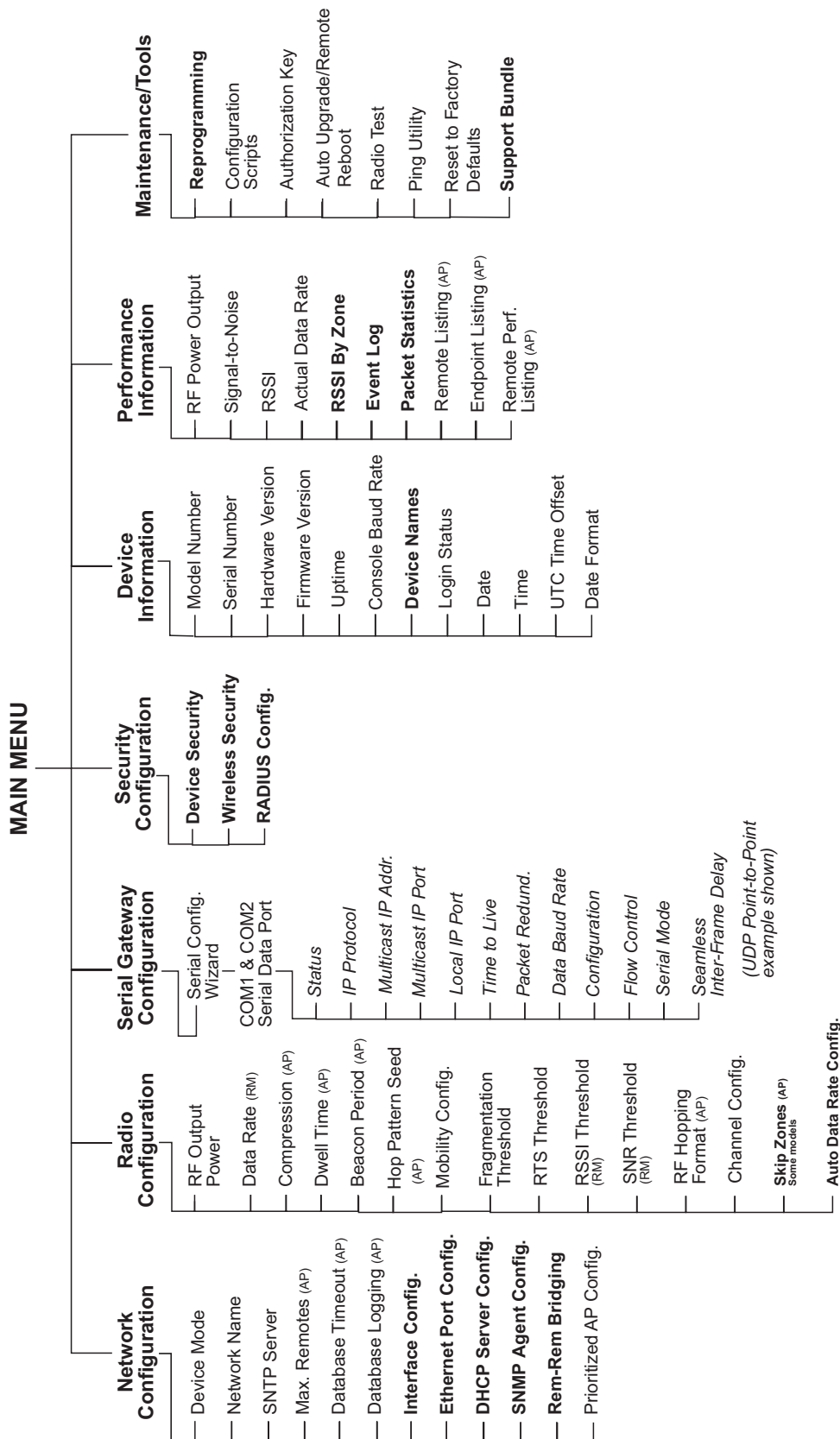
The transceiver's embedded management system is accessible through various data interfaces. These include the COM1 (serial) port, LAN (Ethernet) port, and via SNMP. Essentially the same capabilities are available through any of these paths.

For SNMP management, the transceiver is compatible with MDS *PulseNET* software. Refer to the documentation provided with the software. For support of other SNMP software, a set of MIB files is available for download from the GE MDS Web site at www.gedigitalenergy.com/Communications. A brief summary of SNMP commands can be found at section 2.4.5 on page 36 of this manual.

The transceiver's Management System and its functions are divided into the following menu groups:

- “Basic Device Information” on Page 22
- “Login Status Menu” on Page 27
- “Radio Configuration” on Page 40
- “Configuring the Serial Ports” on Page 49
- “Cyber Security Configuration” on Page 64
- “Performance Verification” on Page 69
- “Maintenance” on Page 82

Each of these sections has a focus that is reflected in its heading. The section you are now reading provides information on connecting to the Management System, how to navigate through it, how it is structured, and how to perform top-level configuration tasks. Figure 2-1 on the following page shows a top-level view of the Management System (MS).



- Bolded items indicate a menu selection
- Spacebar used to make some menu selections
- AP = Access Point Only
- RM = Remote Only

NOTES

- Chart shows top-level view only. Details are given on the following pages.
- Not all items are user-configurable
- Some menu items depend on the Device Mode selected

Figure 2-1. Embedded Management System—Top-level Flowchart

2.1.1 Differences in the User Interfaces

There are slight differences in navigation, but for the most part, the content is the same among different user interfaces. You will find a few differences in capabilities as the communications tool is driven by limitations of the access channel. Figure 2-2 and Figure 2-3 on Page 16 provide examples of the Starting Information Screen seen through a terminal and a Web-browser, respectively.

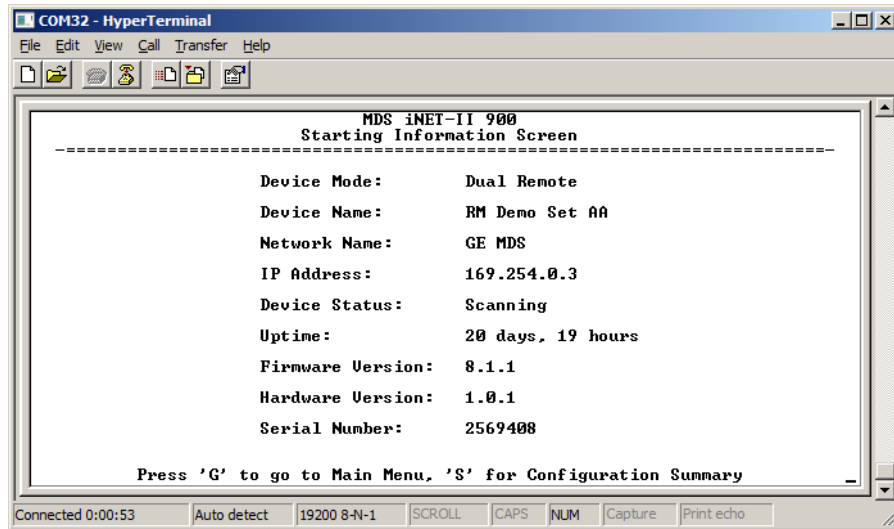


Figure 2-2. View of MS with a text-based program—
(Terminal Emulator shown—Telnet has similar menu structure)

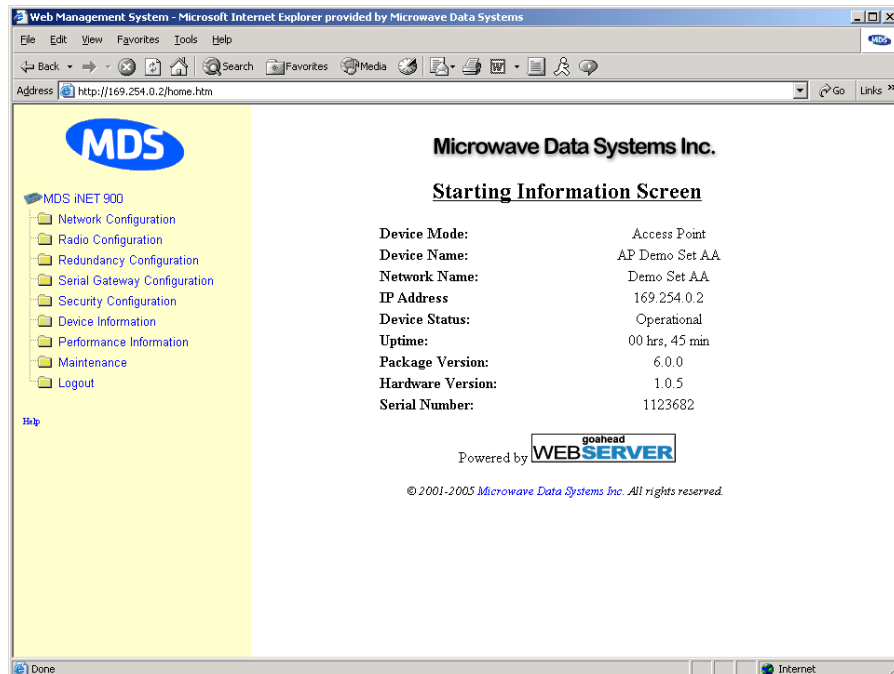


Figure 2-3. View of the MS with a Browser
(Selections at left provide links to the various menus)

2.2 Accessing the Menu System

The radio has no external controls. All configuration, diagnostics and control is performed electronically using a connected PC. This section explains how to connect a PC, log into the unit, and gain access to the built-in menu screens.

2.2.1 Methods of Control

The unit's configuration menus may be accessed in one of several ways:

- **Local Console**—*This is the primary method used for the examples in this manual.* Connect a PC directly to the COM 1 port using a serial communications cable and launch a terminal communications program such as HyperTerminal. This method provides text-based access to the unit's menu screens. Console control is a hardware-based technique, and is intended for local use only.
- **Telnet or SSH***—Connect a PC to the unit's LAN port, either directly or via a network, and launch a Telnet session. This method provides text-based access to the unit's menu screens in a manner similar to a Local Console session. Telnet sessions may be run locally or remotely through an IP connection.
- **Web Browser***—Connect a PC to the unit's LAN port, either directly or via a network, and launch a web browser session (*i.e.*, Internet Explorer, Firefox, etc.) This method provides a graphical representation of each screen, just as you would see when viewing an Internet website. The appearance of menu screens differs slightly from other methods of control, but the content and organization of screen items is similar. Web browser sessions may be run locally or remotely via the Internet.

* Telnet, SSH and Web Browser sessions require the use of a *straight-through* or *crossover* Ethernet cable, depending on the whether the PC-to-radio connection is made directly, or through an Ethernet switch. For direct connection, a **crossover** cable is required; For connection using an Ethernet switch, a **straight-through** type is needed.

Cable type can be identified as follows: Hold the two cable ends side-by-side and in the same plug orientation (*i.e.*, both locking tabs up or down). Now look at the individual wire colors on each plug. If the wires on both plugs are ordered in the same sequence from left to right, the cable is a straight-through type. If they are not in the same order, it *may* be a crossover cable, or it may be wired for some other application. Refer to “**Data Interface Connectors**” on Page 124 for detailed pinout information.

2.2.2 PC Connection & Log In Procedures

The following steps describe how to access the radio's menu system. These steps require a PC to be connected to the unit's COM 1 or LAN port as shown in Figure 2-4.

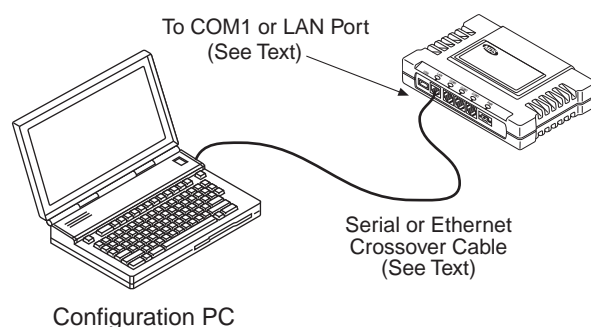


Figure 2-4. PC Configuration Setup

Starting a Local Console Session (Recommended for first-time log-in)

1. Connect a serial communications cable between the PC and the unit's COM 1 port. If necessary, a cable may be constructed for this purpose as shown in Figure 2-5.

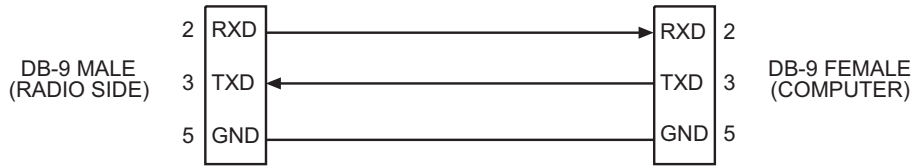


Figure 2-5. Serial Communications Cable (DB-9 to DB-9)
(Maximum Recommended Cable Length 50 Feet/15 meters)

2. Launch a terminal emulation program such as HyperTerminal and configure the program with the following settings:

- 19,200 bps data rate
- 8 data bits, no parity
- One stop bit, and no flow-control
- Use ANSI or VT100 emulation.

TIP: The HyperTerminal communications program can be accessed on most PCs by selecting this menu sequence: **Start>>Programs>>Accessories>>Communications>>HyperTerminal**.

NOTE: Early versions of PuTTY might not operate when using SSH to connect to the transceiver. However, beta versions 0.59 and later do work properly. Both the latest released and the latest development snapshot can be downloaded from:
www.chiark.greenend.org.uk/~sgtatham/putty/.

NOTE: If the unit is powered-up or rebooted while connected to a terminal, you will see a series of pages of text information relating to the booting of the unit's microcomputer. Wait for the log-in screen before proceeding.

3. Press the **[ENTER]** key to receive the **login:** prompt.

4. Enter the username, if applicable (default username is **iNET** or **iNET-II**, in accordance with radio model). Press **[ENTER]**.

5. Enter your password (default password is **admin**). (For security, your password keystrokes do not appear on the screen.) Press **[ENTER]**.

NOTE: Passwords are case sensitive. Do not use punctuation mark characters. You may use up to eight alpha-numeric characters.

The unit responds with the Starting Information Screen (Figure 2-6). From here, you can review basic information about the unit or press **G** to proceed to the Main Menu.

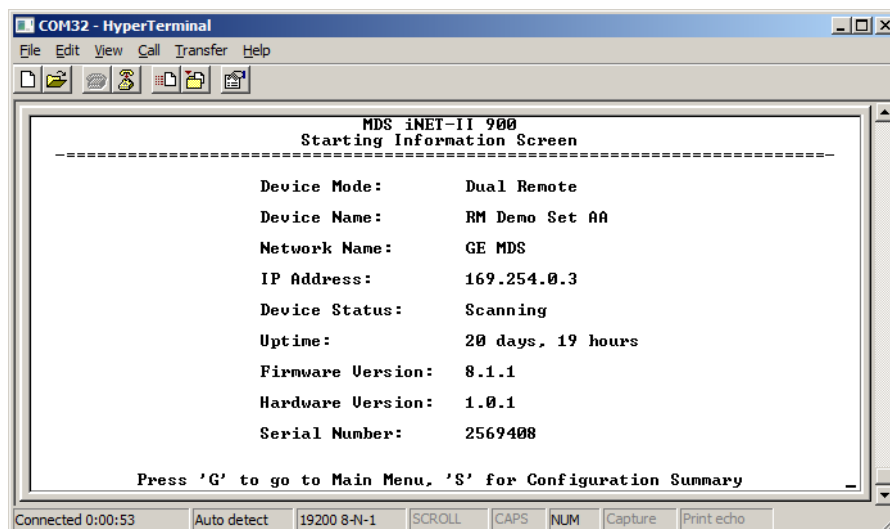


Figure 2-6. Starting Information Screen—Local Console Session
(Telnet has similar menu structure)

Starting a Telnet Session

NOTE: This method requires that you know the IP address of the unit beforehand. If you do not know the address, use the Local Console method (above) and access the *Starting Information Screen*. The address is displayed on this screen.

1. Connect a PC to the unit's LAN port, either directly or via a network. If connecting directly, use an Ethernet *crossover* cable; if connecting via a network, use a *straight-through* cable. The LAN LED lights to indicate an active connection.

NOTE: When using Ethernet to access the unit, it may be necessary to change your computer's IP address to be compatible with the radio IP address. You can identify or verify the unit's IP address by using a Local Console session to communicate with the radio through its COM 1 Port and viewing the *Starting Information Screen*.

2. Start the Telnet program on your computer targeting the IP address of the unit to which you are connected. and press **[ENTER]**.

TIP: A Telnet session can be started on most PCs by selecting: **Start>>Programs>>Accessories>>Command Prompt**. At the command prompt window, type the word **telnet**, followed by the unit's IP address (*e.g.*, **telnet 10.1.1.168**). Press **[ENTER]** to receive the Telnet log in screen.

NOTE: Never connect multiple units to a network with the same IP address. Address conflicts will result in improper operation.

3. Enter your username, if applicable (default username is **iNET** or **iNET-II**, in accordance with radio model). Press **[ENTER]**.

Next, the **Password:** prompt appears. Enter your password (default password is **admin**). (For security, your password keystrokes will not appear on the screen.) Press **[ENTER]**.

The unit responds with a Starting Information Screen (see Figure 2-6). From here, you can review basic information about the unit or press **G** to proceed to the Main Menu.

NOTE: Passwords are case sensitive. Do not use punctuation mark characters. You may use up to eight alpha-numeric characters.

Starting a Web Browser Session

NOTE: Web access requires that you know the IP address of the unit you are connecting to. If you do not know the address, start a Local Console session (see *Starting a Local Console Session (Recommended for first-time log-in)* on Page 17) and access the *Starting Information Screen*. The IP address is displayed on this screen.

1. Connect a PC to the unit's LAN port, either directly or via a network. If connecting directly, use an Ethernet *crossover* cable; if connecting via a network, use a *straight-through* cable. The LAN LED lights to indicate an active connection.
2. Launch a Web-browser session on your computer (*i.e.*, Internet Explorer, Firefox, etc.).
3. Type in the unit's IP address and press **ENTER**.
4. A log-in screen is displayed (Figure 2-7) where you enter a user name and password to access the unit's menu system. (Default username is **iNET** or **iNET-II**, in accordance with radio model; Default Password is **admin**).

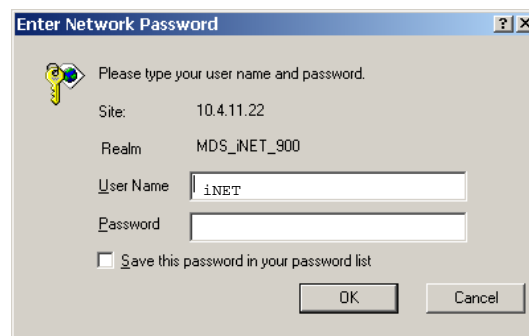


Figure 2-7. Log-in Screen—Web Browser Example

NOTE: Passwords are case sensitive. Do not use punctuation mark characters. You may use up to eight alpha-numeric characters.

5. Click **OK**. The unit responds with a startup menu screen similar to that shown in Figure 2-8. From here, you can review basic information about the unit or click on one of the menu items at the left side of the screen.

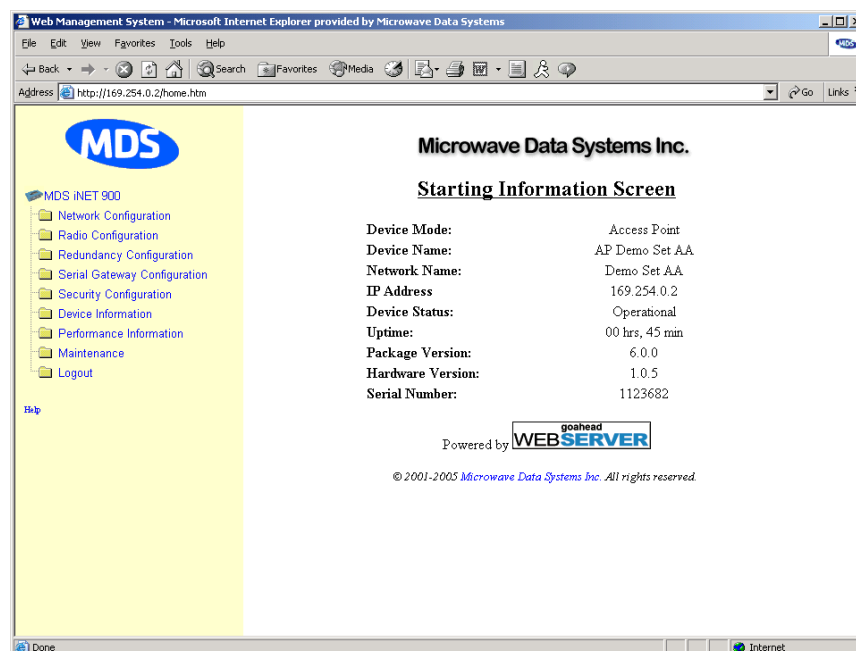


Figure 2-8. Starting Information Screen—Web Browser Example

2.2.3 Navigating the Menus

Via Terminal Telnet or SSH Sessions

Recommended for first-time log-in

Local Console Telnet and SSH sessions use multi-layered text menu systems that are nearly identical. To move further down a menu tree, you type the letter assigned to an item of interest. This takes you to an associated screen where settings may be viewed, or changed. In most cases, pressing the **[ESCAPE]** key moves the screen back one level in the menu tree.

In general, the top portion of menu screens show *read-only* information (with no user selection letter). The bottom portion of the screen contains parameters that can be selected for further information, alteration of values, or to navigate to other submenus.

When you arrive at a screen with user-controllable parameter fields, you select the menu item by pressing an associated letter on the keyboard. If there is a user definable value, the field will clear to the right of the menu item and you can type in the value you wish to use. Follow this action by pressing the **[ENTER]** key to save the changes. If you make a mistake or change your mind before pressing the **[ENTER]** key, simply press **[ESCAPE]** to restore the previous value.

In some cases, when you type a letter to select a parameter, you will see a prompt at the bottom of the screen that says **Choose an Option**. In these screens, press the keyboard's **[SPACEBAR]** to step through the available selections. When the desired option appears, press the **[ENTER]** key to choose that selection. In some cases, several parameters may be changed and then saved by a single keystroke. The **[ESCAPE]** key can be used to cancel the action and restore the previous values.

Logging Out Via Terminal Emulator or Telnet

From the Main Menu screen, press **Q** to quit and terminate the session.

Navigating via Web Browser

Navigating with a Web browser is straightforward with a framed “homepage.” The primary navigation menu is permanently located on the left-hand side of this page. Simply click on a desired menu item to bring it to the forefront.

NOTE: To maintain security, it is best to log-out of the menu system entirely when you are done working with it.

Logging Out Via Web Browser

Click on **Logout** in the left-hand frame of the browser window. The right-hand frame will change to a logout page. Follow the remaining instructions on this screen.

NOTE: In the menu descriptions that follow, parameter options/range, and any default values are displayed at the end of the text between square brackets. Note that the default setting is always shown after a semicolon: [available settings or range; default setting]

2.3 Basic Device Information

This section contains detailed menu screens and settings that you can use to specify the behavior of the unit.

2.3.1 Starting Information Screen

Once you have logged into the Management System, you will be presented with a screen that provides an overview of the transceiver and its current operating condition. It provides an array of vital information and operating conditions.

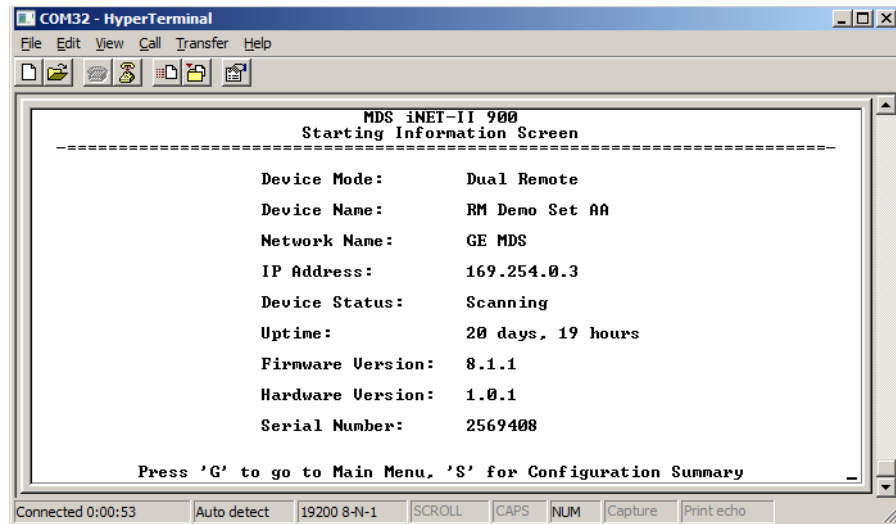


Figure 2-9. Starting Information Screen

- **Device Mode**—Current operating mode of the unit as it relates to the radio network. [Access Point, Dual Remote, Serial Remote, Ethernet Remote]
- **Device Name**—This is a user-defined parameter that will appear in the heading of all pages. (To change it, see “Network Configuration Menu” on Page 27.)

NOTE: Do not use a colon (:) or percent (%) symbol in the device name.

- **Network Name**—The name of the radio network in which the unit is associated [9 to 15 characters; Not Programmed].
-

- **IP Address**—Unit's IP address [192.168.1.1]
- **Device Status**—Condition of the unit's association with an Access Point. During an alarmed state, the radio will display *Alarmed* and the current connection status.

At the Access Point:

- *Alarmed*—A alarm event has been logged and not cleared.
- *Operational*—Unit operating normally.

At a Remote:

- *Scanning*—The unit is looking for an Access Point beacon signal.
- *Exp(ecting) Sync(hronization)*—The unit has found a valid beacon signal for its network.
- *Hop Sync*—The unit has changed its frequency hopping pattern to match that of the Access Point.
- *Connected*—The unit has established a radio (RF) connection with the Access Point, but has not obtained cyber-security clearance to pass data.
- *Associated*—This unit has successfully synchronized and associated with an Access Point.
- *Alarmed*—The unit has detected one or more alarms that have not been cleared.

NOTE: If an alarm is present when this screen is displayed, an “A” appears to the left of the **Device Status** field. Pressing the “A” key on your keyboard takes you directly to the “Current Alarms” screen.

- **Uptime**—Elapsed time since the transceiver was powered-up.
- **Firmware Version**—Version of firmware that is currently active in the unit.
- **Hardware Version**—Hardware version of the transceiver's printed circuit board.
- **Serial Number**—Make a record of this number. It must be provided to purchase Authorization Keys to upgrade unit capabilities. (See “Authorization Key Menu” on Page 89.)
- **Configuration Summary**—High-level view of configured system parameters. This shows parameters that are currently enabled or being used. View Figure 2-10 below and Figure 2-11 on Page 24 for details.

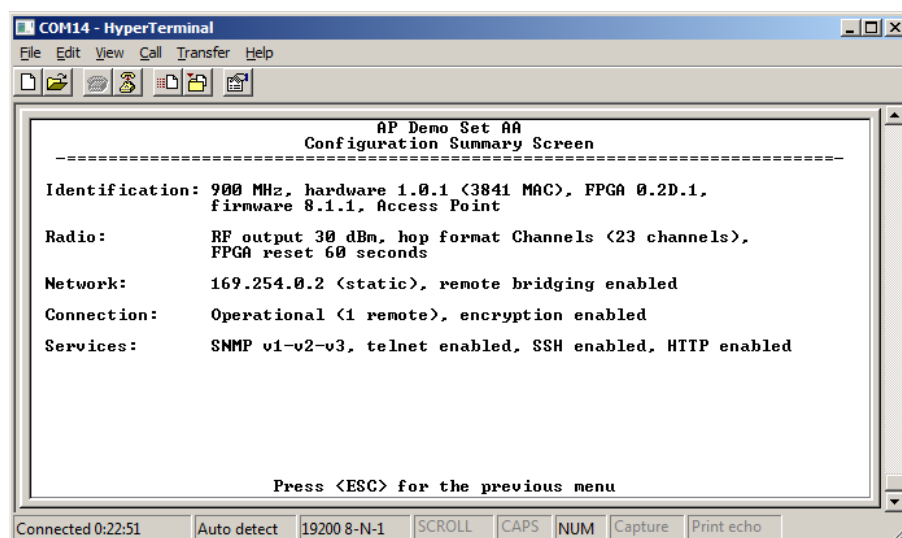


Figure 2-10. Configuration Summary Screen (iNET-II AP)

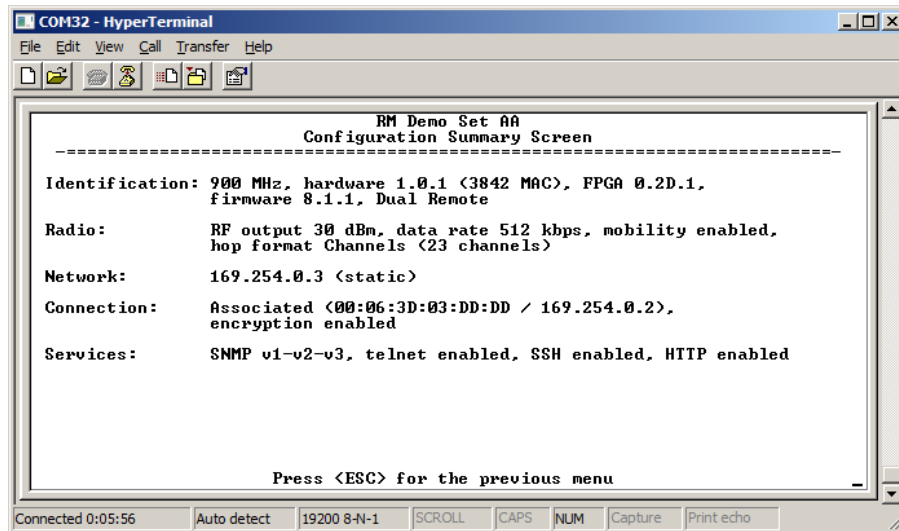


Figure 2-11. Configuration Summary Screen (iNET-II Remote)

- **Identification**—General radio information; frequency, hardware version, FPGA version, firmware version, radio mode, redundancy status.
- **Radio**—Radio configuration; RF power, data rate (RM only), hop format, mobility status (RM only), compression status, FPGA reset timer (AP only), beacon learning status (iNET-II Remote only), prioritized AP (RM only).
- **Network**—Network configuration; IP address (static or DHCP), VLAN status, remote bridging status (AP only), Spanning Tree Protocol status, Ethernet filtering status.
- **Connection**—Over-the-air link status; device status, encryption status, device auth status.
- **Services**—Active services on radio; SNMP status and version, Telnet status, SSH status, HTTP/HTTPs status, DHCP server status, auto upgrade status.

2.3.2 Main Menu

The next screen, the Main Menu, is the entryway to all user-controllable features. The transceiver's **Device Name** appears at the top of this and all other screens as a reminder of the unit that is currently being controlled

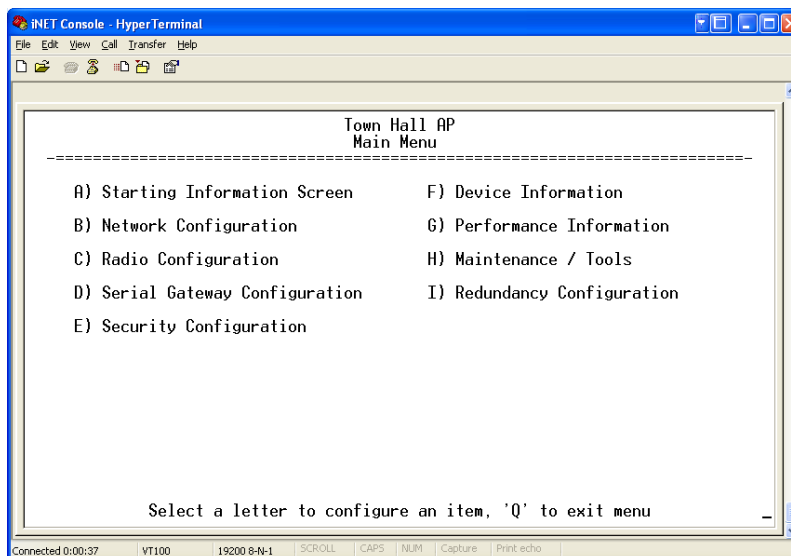


Figure 2-12. Main Menu

- **Starting Information Screen**—Select this item to return to the start-up screen. (See “Starting Information Screen” on Page 22)
- **Network Configuration**—Tools to configure the data network layer of the transceiver. (See “Network Configuration Menu” on Page 27)
- **Radio Configuration**—Tools to configure the wireless (radio) layer of the transceiver. (See “Radio Configuration Menu” on Page 40)
- **Serial Gateway Configuration**—Tools to configure the two serial ports. (See “Serial Data Port Configuration Menu” on Page 51)
- **Security Configuration**—Tools to configure the security services available with the transceiver’s environment. (See “Cyber Security” on Page 11 and see “*Cyber Security Configuration*” on Page 64)
- **Device Information**—Top level user-specific and definable parameters, such as the device name. (See “Device Information” on Page 25)
- **Performance Information**—Tools to measure the radio and data layer’s performance of the radio network. (See “Performance Verification” on Page 69)
- **Maintenance/Tools**—Tools to use configuration files, change firmware and use Authorization Keys to change major unit capabilities. (See “Maintenance” on Page 82 and see “*Authorization Key Menu*” on Page 89)
- **Redundancy Configuration**—For operation in protected (redundant) mode. The radio must be in a P21 enclosure for this operation. See publication 05-4161A01 for details, available under the Downloads tab at www.gemds.com.

NOTE: Standard MDS iNET (non-iNET-II) transceivers require special firmware to operate in redundant mode. See “Upgrading the Firmware” on Page 84 for details.

2.3.3 Configuring Basic Device Parameters

Device Information

Below is the menu/screen that displays basic administrative data on the unit to which you are connected. It also provides access to some user- specific parameters such as device names.

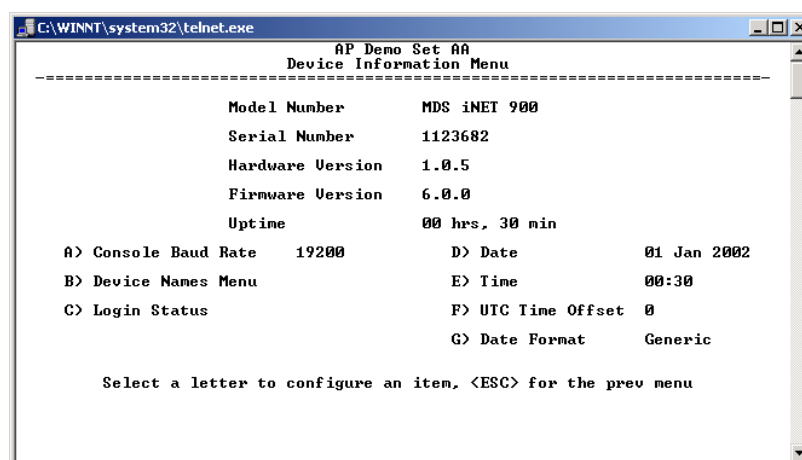


Figure 2-13. Device Information Menu

- **Model Number** (*Display only*)
- **Serial Number** (*Display only*)
- **Hardware Version** (*Display only*)
- **Firmware Version** (*Display only*)—Current firmware installed and being used by the transceiver.
- **Uptime** (*Display only*)—Elapsed time since powering up.
- **Console Baud Rate**—Used to set/display data communications rate (in bits-per-second) between a connected console terminal and the radio. [1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200; 19200]

- **Device Names Menu**—Fields used at user’s discretion for general administrative purposes. The Device Name field is used by the transceiver as the “Realm” name for network security and in the MS screen headings. (See Figure 2-14 on Page 26)

NOTE: Do not use a colon (:) or percent (%) symbol in the device name.

- **Login Status**—Shows active login sessions to the radio’s local or remote console.
- **Date**—Current date being used for the transceiver logs. User-settable. (Value lost with power failure if SNTP (Simple Network Time Protocol) server not accessible.)
- **Time**—Current time of day. User-settable.
Setting: HH:MM
(Value lost with power failure if SNTP server not accessible.)
- **Date Format**—Select presentation format:
 - Generic = dd Mmm yyyy
 - European = dd-mm-yyyy
 - US = mm-dd-yyyy

Device Names Menu

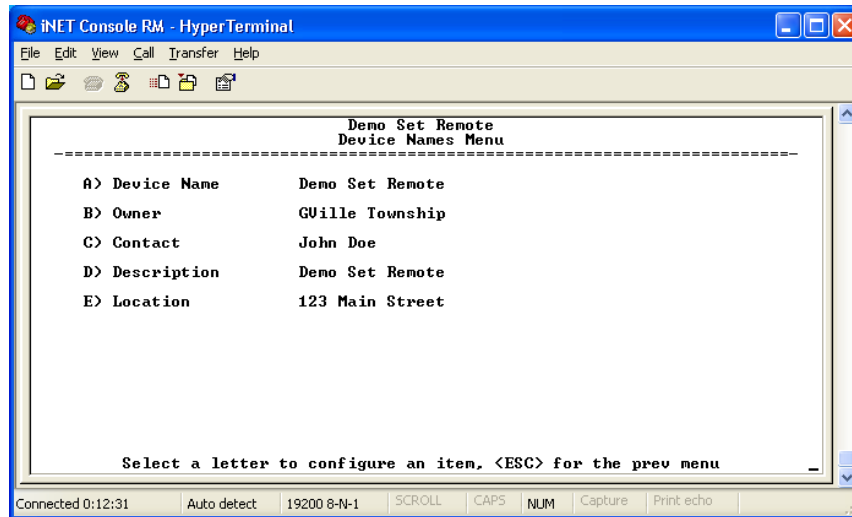


Figure 2-14. Device Names Menu

- **Device Name**—Device Name, used by the transceiver as the “Realm” name for network login (web browser only) and menu headings.

NOTE: Do not use a colon (:) or percent (%) symbol in the device name.

- **Owner**—User defined; appears on this screen only.
- **Contact**—User defined; appears on this screen only.
- **Description**—User defined; appears on this screen only.
- **Location**—User defined; appears on this screen only.

Login Status Menu

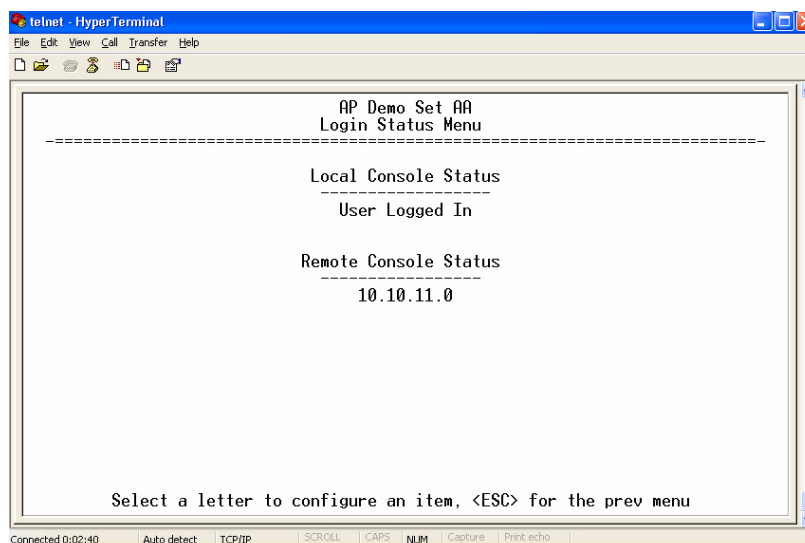


Figure 2-15. Login Status Menu

- **Local Console Status**—Read only display indicating if the local console session is being used (serial console).
- **Remote Console Status**—Read only display that shows the IP address of the endpoint connected via the Remote Console (telnet).

2.4 Configuring Network Parameters

2.4.1 Network Configuration Menu

This Menu contains parameters related to the operation of TCP/IP and Ethernet protocols. There are some differences between AP and Remote type radios regarding these parameters and they are noted where appropriate.

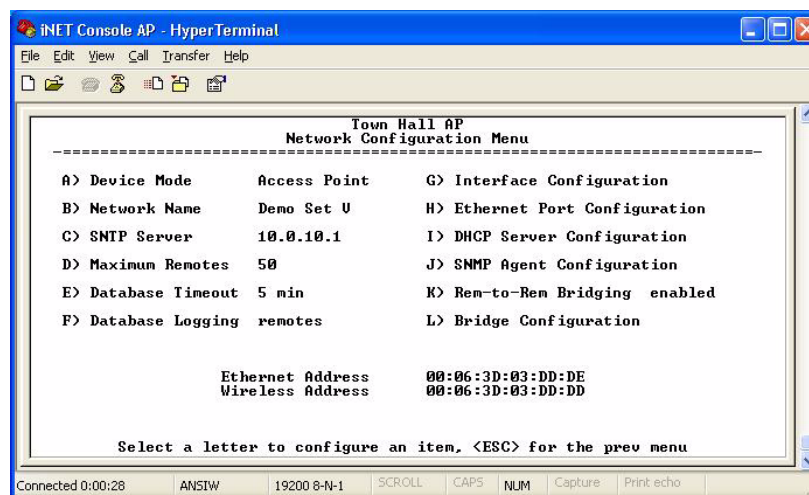


Figure 2-16. Network Configuration Menu
From Access Point

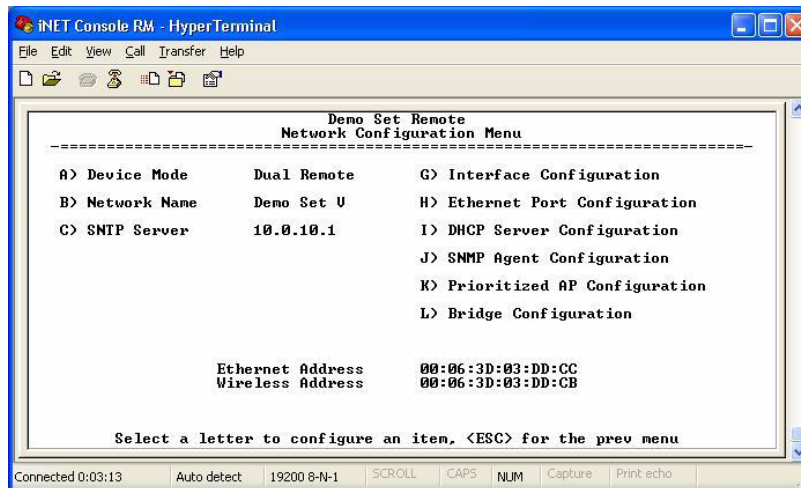


Figure 2-17. Network Configuration Menu
From Remote Unit

- **Device Mode**—Either Access Point or a variation of a Remote. [**Access Point, Remote; Remote**]

NOTE: A serial Remote can be turned into an Ethernet Bridge and vice-versa. See “Change the Type of Remote” on Page 89 for details.

- **Network Name**—Name of the radio network that this unit belongs to. Essential for association of Remotes to the Access Point in a network. The Network Name should be at least nine characters long. [**9 to 15 characters; Not Programmed**]

TIP: For enhanced security, consider using misspelled words, a combination of letters and numbers, and a combination of upper and lower case letters. This helps protect against sophisticated hackers who may use a database of common words (for example, dictionary attacks) to determine the Network Name.

- **SNTP Server**—Address of SNTP server (RFC 2030) from which the transceiver will automatically get the time-of-day startup time. Without an SNTP server, the date and time must be manually set. An AP will try to get the time and date from the SNTP server only if an IP address is configured. It will continue to retry every minute until it succeeds.

A remote will get the time and date from the SNTP server, if an IP address is configured. Otherwise it gets it from the AP at authentication time. The transceivers use UTC (Universal Coordinated Time) with a configurable time offset. [**0.0.0.0**]

- **Maximum Remotes** (AP only)—Number of Remotes permitted to be associated with this Access Point. [**50; 0 to 255**]
- **Database Timeout** (AP Only)—This sets the database “age time.” See “Remote Listing Menu (Access Points Only)” on Page 78 to determine when a remote is declared unavailable. The timer may be set from 0 to 255 minutes and resets each time a message is received from a remote. [**0–255 minutes; 5 minutes**]
- **Database Logging** (AP Only)—Determines which types of devices will be reported as “added” or “deleted” from the AP’s database (see “*Performance Verification*” on Page 69). In the case of deletions, this information is triggered by the expiration of Database Timeout above. The **Remotes** option only reports the remote radios. Selecting **All** reports endpoints *and* remotes. [**Remotes, All, Disabled; Remotes**].
- **Interface Configuration**—Presents a menu for configuring the Virtual LAN (VLAN) and IP address of the transceiver. Detailed explanations are provided in the section titled “Network Interface Configuration Menu” on Page 29.

NOTE: In MDS iNET radios (where VLAN is not available or is not enabled), this option is shown as **IP ADDRESS CONFIGURATION**. Selecting this option follows the description in “Configuring the IP Address When VLAN Status is Disabled” on Page 32.

- **Ethernet Port Configuration**—Presents a menu for defining the status of the Ethernet port (enabled or disabled), the Ethernet rate limit, link hardware watch (enabled/disabled), and the Ethernet link poll address. Detailed explanations of this menu are contained on Page 33.
- **DHCP Server Configuration**—Menu for configuration of DHCP services. DHCP provides “on-the-fly” IP address assignments to other LAN devices, including MDS iNET 900 units. See “DHCP Server Configuration” on Page 35 for more information.
- **SNMP Agent Configuration**—Contains SNMP configuration parameters. See “SNMP Agent Configuration” on Page 36 for more information.
- **Rem-to-Rem Bridging**—This option is only available on Access Point radios. When this option is disabled communication can only happen from Remote to Access Point. This setting prevents a PC connected to one Remote radio to access a network connected to a different Remote within the same AP realm. [enabled, disabled; enabled]
- **Prioritized AP Configuration**—This option is only available on Remotes. It allows the definition of a Primary AP to which a Remote radio should be connected. See “Prioritized AP Configuration Sub-menu” on Page 38 for more information.
- **Bridge Configuration**—View/set options for Spanning Tree and Ethernet Bridge operation. See “When a beacon matches the requirements, then the association process continues. It may be that the Remote associates to an AP that is not the first entry in the table. In this case the Remote will wait for Connection Time before breaking the connection and starting the process all over again. This process will be repeated until the Remote associates to the first entry in the list (the Primary Access Point).” on Page 39.
- **Ethernet Address (Display Only)**—Hardware address of the unit’s Ethernet interface.
- **Wireless Address (Display Only)**—Hardware address of the unit’s wireless Ethernet interface.

2.4.2 Network Interface Configuration Menu

Because iNET-II and iNET radios support 802.1Q VLAN, the method for configuring the IP address of a radio may vary depending on whether the VLAN Status option is enabled or not.

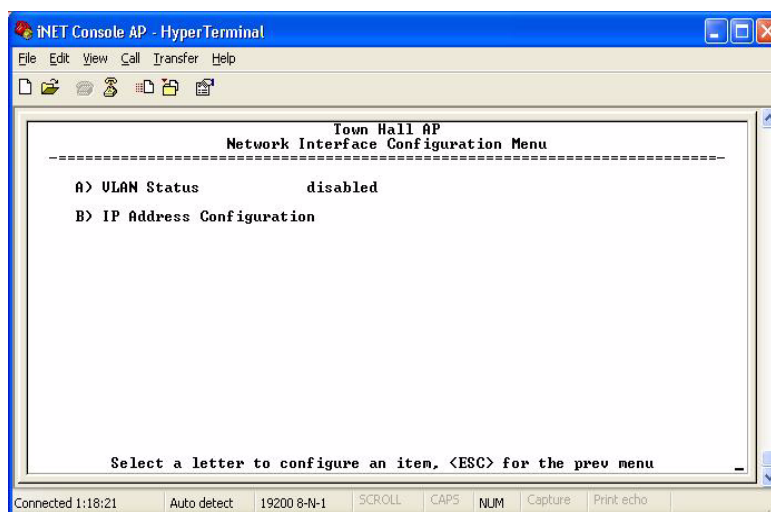


Figure 2-18. Network Interface Configuration Menu

- **VLAN Status**—Defines if the radio handles Ethernet frames in “extended” 802.1Q mode or in “normal” mode in the Ethernet port. [enabled, disabled; disabled]
- **IP Address Configuration**—Allows configuration of IP Addressing parameters. See “Configuring the IP Address when VLAN Status is Enabled” on Page 31, or “Configuring the IP Address When VLAN Status is Disabled” on Page 32.

NOTE: The VLAN Status parameter must be consistent at both Access Point and Remote radios in order for data to flow correctly. Inconsistent configuration may result in improper data flow and the loss of over-the-air communications.

Virtual LAN in iNET Series

The iNET-II and iNET support port-based VLAN at the Ethernet interface and over the air, according to the IEEE 802.1Q standard. A VLAN is a limited broadcast domain, where all members of a VLAN receive frames sent by any other member of the same VLAN but not frames sent by members of a different VLAN. When VLAN Status is enabled, the wireless port of both AP and remote radios always acts as a trunk port.

The Ethernet port of an Access Point radio is normally configured as a trunk port. This type of port expects incoming frames to have a **VLAN ID** and sends outgoing frames with a VLAN structure as well.

- When the Ethernet port of a Remote is configured as a VLAN Access Port, the radio tags incoming traffic with a **VLAN ID**, and strips the tag before sending out traffic. This VLAN is known as the **DATA VLAN**. Additionally, a second VLAN is assigned for other traffic that is terminated at the radio, such as SNMP, TFTP, ICMP, Telnet, etc. This is known as the **MANAGEMENT VLAN**. Traffic directed to the integrated terminal server that handles the serial ports is assigned to the **DATA VLAN**.
- When the Ethernet port of a remote radio is configured as a VLAN trunk, the radio expects all incoming Ethernet frames to be tagged, and passes through all outgoing frames as received from the wireless link, with the unchanged VLAN tag.

NOTE: The Ethernet port in an iNET-II and iNET is 10BaseT. Some Ethernet switches allow a VLAN trunk port only on a 100BaseT interface and may not be able to communicate with the radio.

Configuring for Operation with VLAN

When VLAN Status is enabled the radio uses an 802.1Q frame structure.

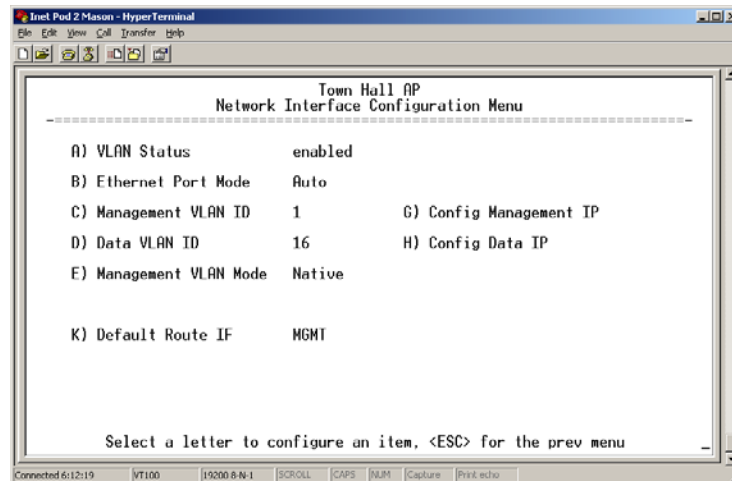


Figure 2-19. Network Interface Configuration Menu

- **VLAN Status**—Defines whether the radio handles Ethernet frames in “extended” 802.1Q mode or in “normal” mode in the Ethernet port. Ethernet frames intended for the radio, but with a VLAN ID not configured in the radio are discarded.
[enabled, disabled; disabled]

NOTE: A change made to the above parameter will result in the Commit Changes option appearing on screen. This will modify the appearance of the screen depending on the option selected.

- **Ethernet Port Mode**—Defines if the Ethernet port acts as a trunk port or as an access port. Auto mode defines the port as an access port in an AP, or a trunk port in a Remote radio. [**Auto, Trunk, Access; Auto**]
- **Management VLAN ID**—Defines the VLAN ID for traffic directed to the radio itself, other than the terminal server process. This VLAN ID is used for filtering and for tagging purposes. [**1-4094; 2**]
- **Data VLAN ID**—Defines the VLAN ID assigned to traffic directed to and from the Ethernet port and the terminal server process in the radio. This VLAN ID is used for filtering and for tagging purposes. [**1-4094; 3**]
- **Config Management IP**—Calls up a menu to configure the IP address associated with the Management VLAN ID.
- **Config data IP**—Calls up a menu to configure the IP address associated with the Data VLAN ID.
- **Default Route IF**—Defines the VLAN that contains the default gateway in the radio. [**MGMT, DATA; MGMT**]

Configuring the IP Address when VLAN Status is Enabled

The radios require a local IP address to support remote management and serial device (terminal server) services. When the radio is configured for VLAN operation the IP address can only be set as a static IP address.

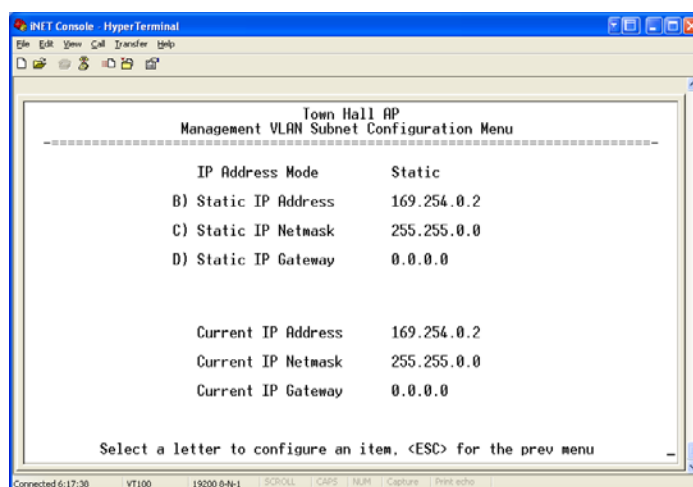


Figure 2-20. Management VLAN Subnet Configuration Menu

- **IP Address Mode**—Defines the source of the IP address of this device. Only static IP addressing mode is available when VLAN Status is enabled.

NOTE: Changes to any of the following parameters while communicating over the network (LAN or over-the-air) may cause a loss of communication with the unit being configured. Communication will need to be re-established using the new IP address.

- **Static IP Address**—The IPv4 local IP address. [**192.168.1.1**]
- **Static IP Netmask**—The IPv4 local subnet mask. This value is used when the radio attempts to send a locally initiated message, either from the terminal server, or management process. [**255.255.0.0**]
- **Static IP Gateway**—The IPv4 address of the default gateway device, typically a router. [**0.0.0.0**]

The lower three lines of the screen show the current addressing configured at the transceiver.

NOTE: Any change made to the above parameters results in the **Commit Changes** option appearing on screen. This allows all IP settings to be changed at the same time.

Selecting option H from Figure 2-19 shows Figure 2-21. Note that the IP address is different although it is the same physical unit. This is because this IP address is defined for a different VLAN.

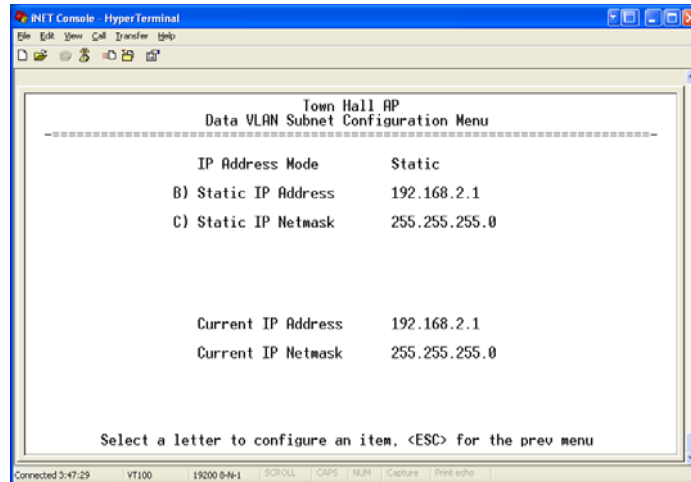


Figure 2-21. Data VLAN Subnet Configuration Menu

- **IP Address Mode**—Defines the source of the IP address of this device. Only static IP addressing mode is available when VLAN Status is enabled.

NOTE: Changes to any of the following parameters while communicating over the network (LAN or over-the-air) may cause a loss of communication with the unit being configured. Communication will need to be re-established using the new IP address.

- **Static IP Address**—The IPv4 local IP address. [192.168.1.1]
- **Static IP Netmask**—The IPv4 local subnet mask. This value is used when the radio attempts to send a locally initiated message, either from the terminal server, or management process. [255.255.0.0]

Configuring the IP Address When VLAN Status is Disabled

When the radio is not configured for operation with VLAN, it uses one IP address to support remote management and serial device services. The IP address of a radio can be set as a static IP address or as a dynamic IP address. When static IP addressing is used, the user must manually configure the IP address and other parameters. When dynamic addressing is used, the radio uses a DHCP Client process to obtain an IP address from a DHCP Server, along with other parameters such as a subnet mask and a *default gateway*.

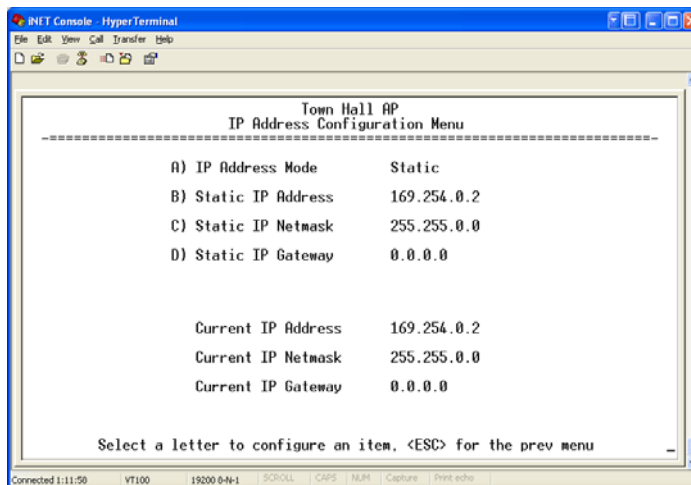


Figure 2-22. IP Address Configuration Menu

CAUTION: Changes to any of the following parameters while communicating over the network (LAN or over-the-air) may cause a loss of communication with the unit being configured. Communication will need to be re-established using the new IP address.

- **IP Address Mode**—Defines the source of the IP address of this device. The IP address must be configured manually when set to Static. A DHCP server must be available for the radio to obtain a valid IP address when set to Dynamic. Enabling this option forces the transceiver (AP or Remote) to obtain an IP address from any DHCP server available on the LAN. Dynamic Mode is also known as DHCP Client mode. Only static IP addressing mode is available when VLAN Status is enabled [**Static; Static, Dynamic**].
- **Static IP Address**—The IPv4 local IP address. It need not be defined if DHCP Client mode is enabled. [192.168.1.1]
- **Static IP Netmask**—The IPv4 local subnet mask. This value is used when the radio attempts to send a locally initiated message, either from the terminal server, or management process. You don't have to define it if DHCP Client mode is enabled. [255.255.0.0]
- **Static IP Gateway**—The IPv4 address of the default gateway device, typically a router. [0.0.0.0]

The lower three lines of the screen show the actual addressing at the transceiver, whether it was obtained from static configuration or from a DHCP server.

NOTE: Any change made to the above parameters results in the **Commit Changes** option appearing on screen. This allows all IP settings to be changed at the same time.

2.4.3 Ethernet Port Configuration Menu

The transceiver allows for special control of the Ethernet interface, to allow traffic awareness and availability of the backhaul network for redundancy.

NOTE: The Ethernet port in iNET and iNET-II radios support 10BaseT connections only. This should not present a problem because most hubs/switches auto-switch between 10BaseT and 100BaseT connections. Confirm that your hub/switch is capable of auto-switching data rates.

To prevent Ethernet traffic from degrading performance, place the transceiver in a segment, or behind routers.

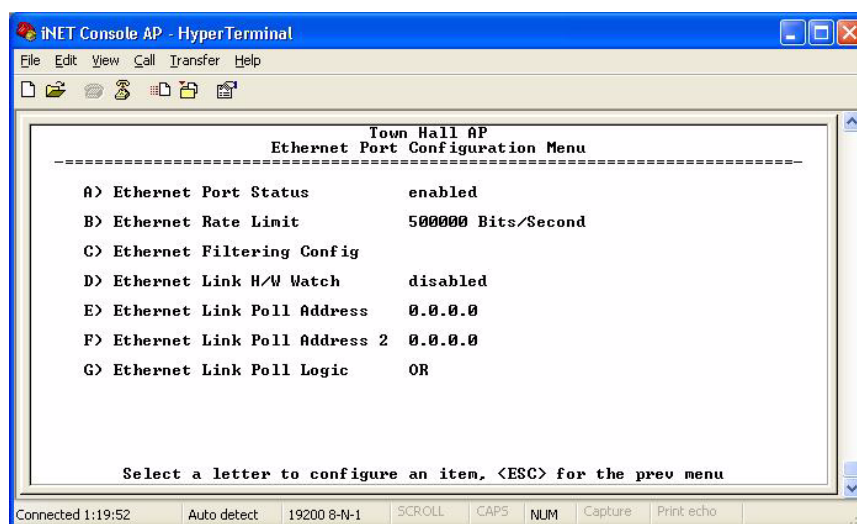


Figure 2-23. Ethernet Port Configuration Menu
(AP menu shown; Remote omits items D through G)

- **Ethernet Port Status**—Allows enabling/disabling Ethernet traffic for security purposes. Setting it to **Follow Radio Link** on the Remote enables the port if there is a connection established with the AP, but disables it otherwise. [AP: **Enabled, Disabled; Enabled**. Remote: **Always On, Follow Radio Link, Disabled; Always On**.]
- **Ethernet Rate Limit**—The transceiver will send alarms (SNMP traps) when the rate reaches 50%, 75%, and 100% to help identify potential problems with traffic. [1 to 500000 iNET; 1 to 1000000 iNET-II; 500000 bits/sec]
- **Ethernet Filtering Configuration Menu** (Figure 2-24)—This selection brings up a submenu for defining which Ethernet devices will be “listened to” for forwarding of data packets into the wireless network. When **Ethernet Filtering** is enabled, only packets from listed Ethernet addresses will be forwarded. Up to four addresses may be specified.

This feature—also known as *MAC Address Filtering* is typically used at Remote radios to guard against unwanted traffic being forwarded into the wireless network.

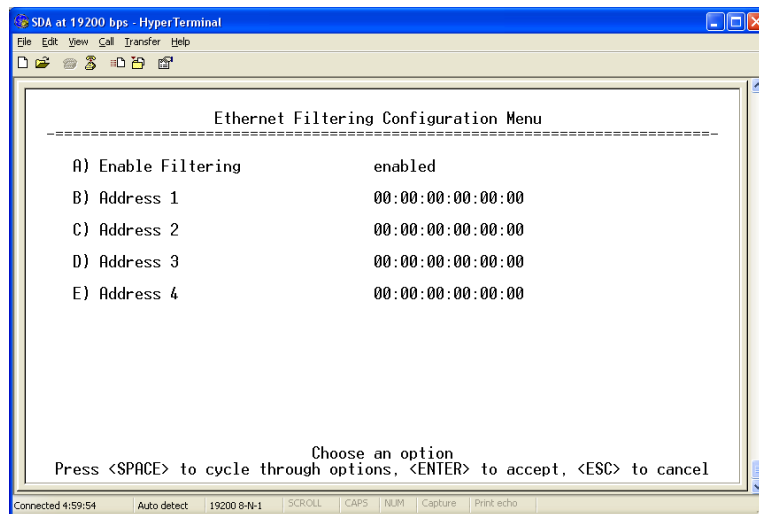


Figure 2-24. Ethernet Filtering Configuration Menu

- **Ethernet Link H/W Watch** (*AP Only*)—Detects the lack of an Ethernet connection to the LAN port at the electrical level (link integrity). The current AP will broadcast a beacon signal indicating its “NOT AVAILABLE” status so Remotes that hear it do not try to associate to it. Once the Ethernet connection is restored, this beacon signal changes to “AVAILABLE” and Remotes are allowed to join in. [Disabled; Enabled, Disabled]
- **Ethernet Link Poll Address / 2** (*AP Only*)—When an IP address is provided, the Access Point pings the remote IP device every 60 seconds to test the integrity of the backhaul link. If this link is not available, the AP will advertise its “NOT AVAILABLE” status in the beacon signal so Remotes do not try to associate to it. Once the IP address is reachable, this beacon signal changes to “AVAILABLE” and Remotes are allowed to join in. 0.0.0.0 disables this function. Any other valid IP address enables it. [0.0.0.0]
- **Ethernet Link Poll Logic** (*AP Only*)—When both Ethernet Link Poll Address options are used, the AP can monitor the two IP addresses separately or together. When using the OR logic, if the AP cannot reach one of the two IP addresses configured, the beacon signal will stay broadcast “AVAILABLE”. Only if both IP addresses cannot be reached will the beacon signal turn to “NOT AVAILABLE” until at least one of the IP addresses responds. Using the AND logic, if one or both of the IP addresses are no longer reachable, the beacon signal will change to “NOT AVAILABLE” until the connectivity returns. [OR; AND, OR]

2.4.4 DHCP Server Configuration

A transceiver can provide automatic IP address assignments to other IP devices in the network by providing DHCP (Dynamic Host Configuration Protocol) services. This service eliminates setting individual device IP address on Remotes in the network, but it still requires thoughtful planning of the IP address range. One drawback to network-wide automatic IP address assignments is that SNMP services may become inaccessible as they are dependent on fixed IP addresses.

The network can be comprised of radios with the DHCP-provided IP address enabled or with DHCP services disabled. In this way, you can accommodate locations for which a fixed IP address is desired.

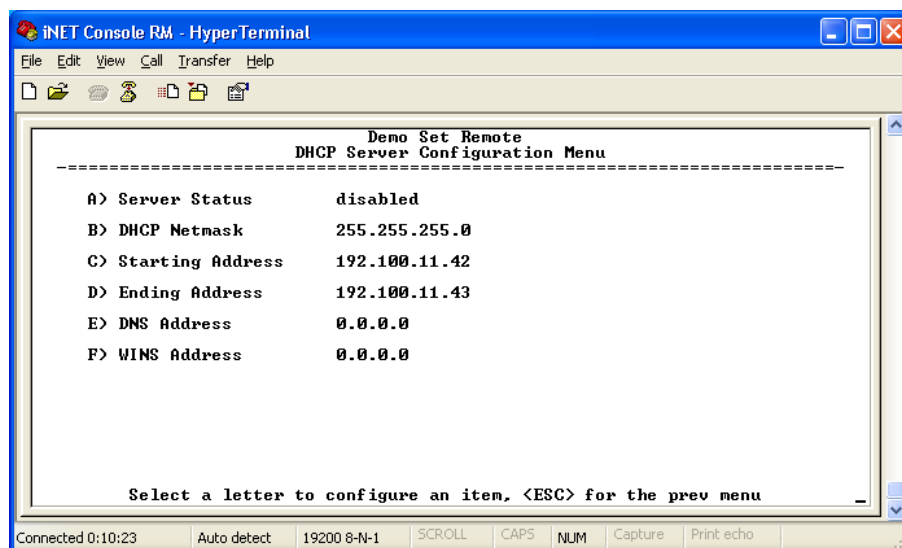


Figure 2-25. DHCP Server Configuration Menu

NOTE: There should be only one DHCP server active in a network (MDS iNET 900 or other DHCP server). If more than one DHCP server exists, network devices may randomly get their IP address from different servers every time they request one.

NOTE: Combining DHCP and RADIUS device authentication may result in a non-working radio module if the DHCP server is located at a remote radio. The DHCP server should be placed at the AP location, if possible.

- **Server Status**—Enable/Disable responding to DHCP requests to assign an IP address. [Disabled/Enabled; Disabled]
- **DHCP Netmask**—IP netmask to be assigned along with the IP address in response to a DHCP request. [0.0.0.0]
- **Starting Address**—Lowest IP address of the range of addresses to be provided by this device. [0.0.0.0]
- **Ending Address**—Highest IP address in the range of addresses to be provided by this device. A maximum of 256 addresses is allowed in this range. [0.0.0.0]
- **DNS Address**—Domain Name Server address to be provided by this service. [0.0.0.0]
- **WINS Address**—Windows Internet Naming Service server address to be provided by this service. [0.0.0.0]

2.4.5 SNMP Agent Configuration

The transceiver contains over 100 custom SNMP-manageable objects as well as the IETF standard RFC1213 for protocol statistics, also known as MIB II. Off-the-shelf SNMP managers such as Castle Rock Computing *SNMPC*™ and Hewlett Packard HP *OpenView*™ may also be used to access the transceiver's SNMP Agent's MIB. The transceiver's SNMP agent supports SNMPv3.

The objects are broken up into several MIB files. There are textual conventions, common files and specific files. This allows the flexibility to change areas of the MIB and not affect other existing installations or customers.

- **msdreg.mib**—GE MDS sub-tree registrations
- **mds_comm.mib**—GE MDS Common MIB definitions for objects and events common to the entire product family
- **inet_reg.mib**—GE MDS sub-tree registrations
- **inetrv1.mib**—SNMPv1 enterprise-specific traps
- **inetrv2.mib**—SNMPv2 enterprise-specific traps
- **inet_com.mib**—MIB definitions for objects and events which are common to the entire iNET Series
- **inet_ap.mib**—MIB definitions for objects and events for an Access Point transceiver
- **inet_sta.mib**—Definitions for objects and events for a Remote radio
- **inet_sec.mib**—For security management of the radio system. SNMPv3 allows read/write operation. SNMPv1/2 allows only for read-only access.
- **inet2.mib**—Additional objects specific to iNET-II.

NOTE: SNMP management requires that the proper IP address, network and gateway addresses are configured in each transceiver of the associated network.

In addition, some management systems may require the MIB files to be compiled in the order shown above.

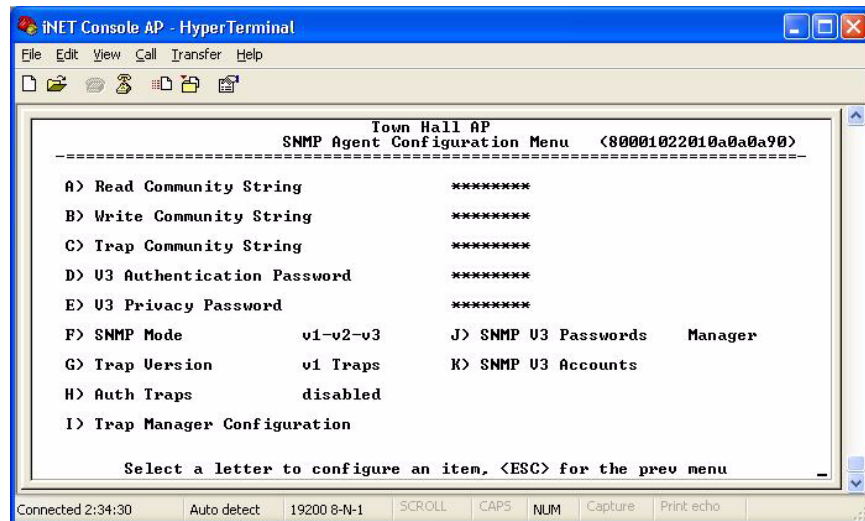


Figure 2-26. SNMP Server Configuration Menu
From Access Point

This menu provides configuration and control of vital SNMP functions.

- **Read Community String**—SNMP community name with SNMPv1/SNMPv2c read access. This string can be up to 30 alpha-numeric characters.
- **Write Community String**—SNMP community name with SNMPv1/SNMPv2c write access. This string can be up to 30 alpha-numeric characters.

- **Trap Community String**—SNMP community name with SNMPv1/SNMPv2c trap access. This string can be up to 30 alpha-numeric characters.
- **V3 Authentication Password**—Authentication password stored in flash memory. This is used when the Agent is managing passwords locally (or initially for all cases on reboot). This is the SNMPv3 password used for Authentication. This string can be up to 30 alpha-numeric characters.
- **V3 Privacy Password**—Privacy password stored in flash memory. Used when the SNMP Agent is managing passwords locally (or initially for all cases on reboot). This is the SNMPv3 password used for privacy (DES encryption). This string can be between 8 and 30 alpha-numeric characters.
- **SNMP Mode**—This specifies the mode of operation of the radio's SNMP Agent. The choices are: disabled, v1_only, v2_only, v3_only, v1-v2, and v1-v2-v3. If the mode is disabled, the Agent does not respond to any SNMP traffic. If the mode is v1_only, v2_only, or v3_only, the Agent responds only to that version of SNMP traffic. If the mode is v1-v2, or v1-v2-v3, the Agent responds to the specified version of SNMP traffic. **[v1-v2-v3]**
- **Trap Version**—This specifies what version of SNMP will be used to encode the outgoing traps. The choices are v1_traps, v2_traps, and v3_traps. When v3_traps are selected, v2-style traps are sent, but with a v3 header. **[v1 Traps, v2 Traps, v3 Traps]**
- **Auth Traps**—Indicates whether or not traps will be generated for login events to the transceiver. **[Disabled/Enabled; Disabled]**
- **Trap Manager Configuration**—Configure where the SNMP traps are sent. See “Trap Manager Submenu” on Page 37.
- **SNMP V3 Passwords**—Determines whether v3 passwords are managed locally or using an SNMP Manager. The Agent behaves differently depending on the mode selected, as described in the SNMP Mode description. **[Manager, Local; Manager]**
- **SNMP V3 Accounts**—Enable or disable SNMP v3 accounts. See “SNMP V3 Accounts Submenu” on Page 38.

NOTE: The number in the upper right-hand corner of the screen is the SNMP Agent's SNMPv3 Engine ID. Some SNMP Managers may need to know this ID in order interface with the transceiver's SNMP Agent. The ID only appears on the screen when SNMP Mode is either v1-v2-v3 or v3_only.

2.4.6 Trap Manager Submenu

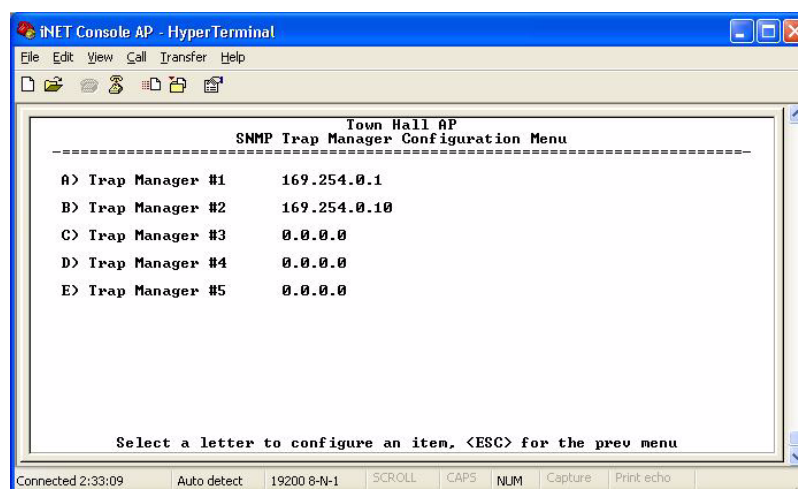


Figure 2-27. SNMP Trap Manager Configuration Menu

Trap Manager #1-5—Configure up to five locations on the network to which traps are sent [Any standard IP address; 0.0.0.0]

2.4.7 SNMP V3 Accounts Submenu

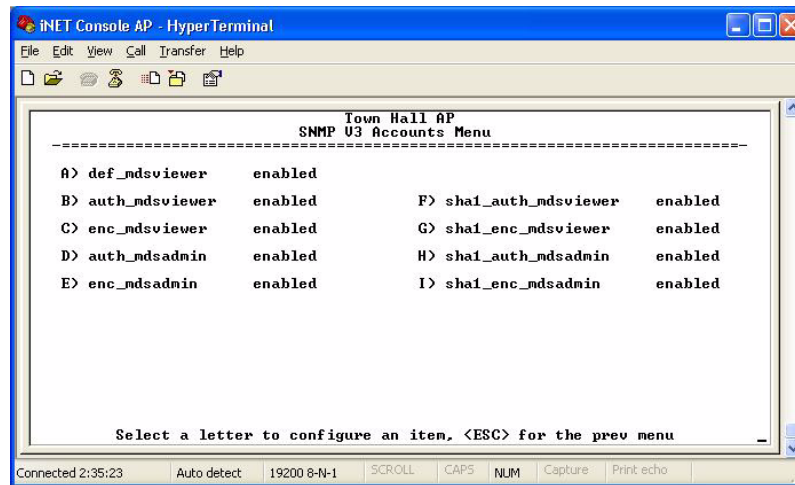


Figure 2-28. SNMP V3 Accounts Menu

This menu allows the user to enable and disable V3 accounts. This secures the radio to avoid unauthorized users access. By default, all v3 accounts are enabled. See “SNMPv3 Accounts” on Page 120 for specific details regarding the access levels of each v3 account.

2.4.8 Prioritized AP Configuration Submenu

The Prioritized AP feature (Figure 2-29) allows the definition of a Primary AP to which a Remote radio should be connected.

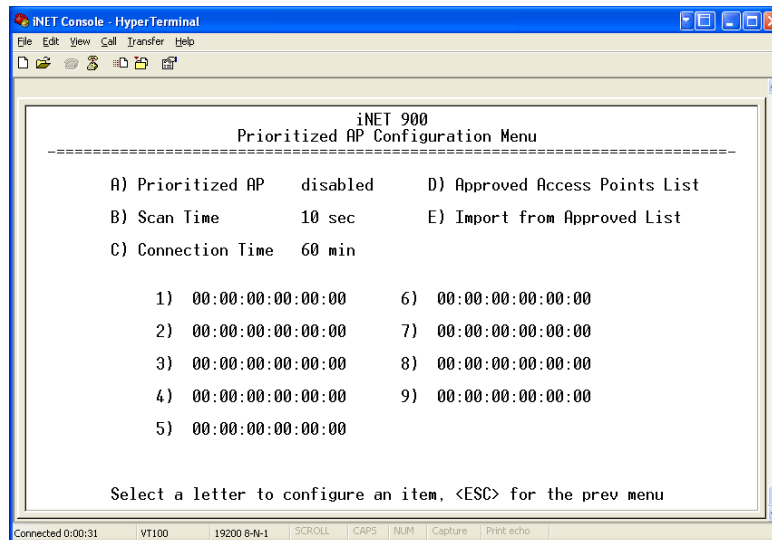


Figure 2-29. Prioritized AP Configuration Submenu

- **Prioritized AP**—Shows status of the prioritization option.
[enabled, disabled; disabled]
- **Scan Time**—Number of seconds that a Remote waits to receive beacons from an AP included in the Approved AP List. After this time, the list will be expanded to include the next entry and the cycle will be repeated until association is achieved.
- **Connection Time**—Amount of time that a Remote waits before breaking the connection and looking for an AP. This event happens only when the current AP is not the first entry in the Approved AP List, which means that the remote is not connected to the primary AP.

- **Approved Access Points List**—Displays the list of Approved AP used for local authentication purposes. This table is not the same as the Priority Table discussed here, and is only included as an aid to facilitate configuration.
- **Import from Approved List**—Copies the entries configured in the Approved AP List to this priority table.
- **1-9**—Priority Table of Access Points. This table should include the Wireless MAC Address of the desired Access Point units.

When association to an AP is terminated for any reason, the Remote enters Scanning mode. During this time it listens for beacons from an AP that matches the network name. If the Prioritized AP option is enabled, then the Wireless MAC Address of the AP must be part of the list at the remote. The initial list includes only the first entry of the table. If no beacon is received that matches the requirement and the Scan Time is exceeded, then the list is expanded to include the first two entries.

When a beacon matches the requirements, then the association process continues. It may be that the Remote associates to an AP that is not the first entry in the table. In this case the Remote will wait for Connection Time before breaking the connection and starting the process all over again. This process will be repeated until the Remote associates to the first entry in the list (the Primary Access Point).

2.4.9 Bridge Configuration Submenu

The Bridge Configuration Menu allows a user to be able to configure Spanning Tree Protocol (STP) functionality and the Ethernet Bridge.

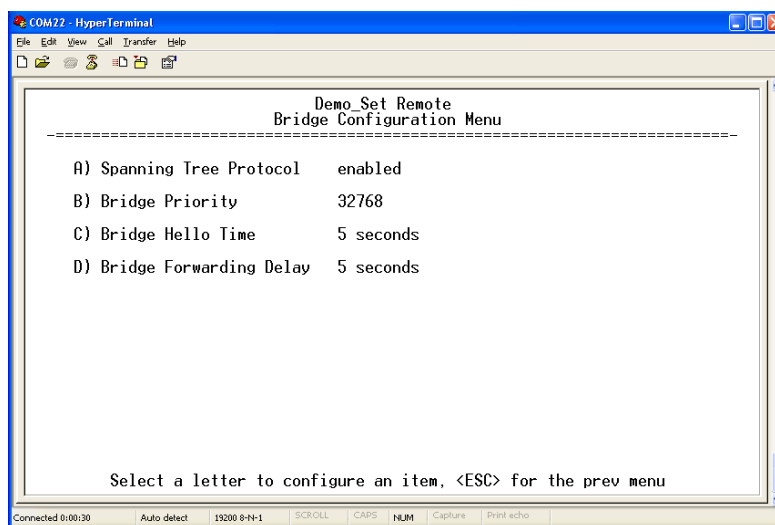


Figure 2-30. Bridge Configuration Submenu

- **Spanning Tree Protocol**—Enable or disable Spanning Tree Protocol (STP) from the unit. **[Enabled, Disabled; Enabled]**
- **Bridge Priority**—View/set the priority of the bridge in the spanning tree. **[0, 65535; 32768]**
- **Bridge Hello Time**—View/set spanning tree hello time. This parameter affects how often the bridge sends a spanning tree Bridge Protocol Data Unit (BPDU) Time between transmissions of Hello messages, in seconds. **[1-10 seconds; 5seconds]**
- **Bridge Forwarding Delay**—View/set spanning tree forwarding delay. Affects how long the bridge spends listening and learning after initialization. **[1-30 seconds; 5 seconds]**

2.5 Radio Configuration

There are two primary data layers in the transceiver network—radio and data. Since the data layer is dependent on the radio layer working properly, configuration of the radio items should be reviewed and set before proceeding. This section explains the *Radio Configuration Menu*, (Figure 2-31 for AP, Figure 2-32 for Remote).

2.5.1 Radio Configuration Menu

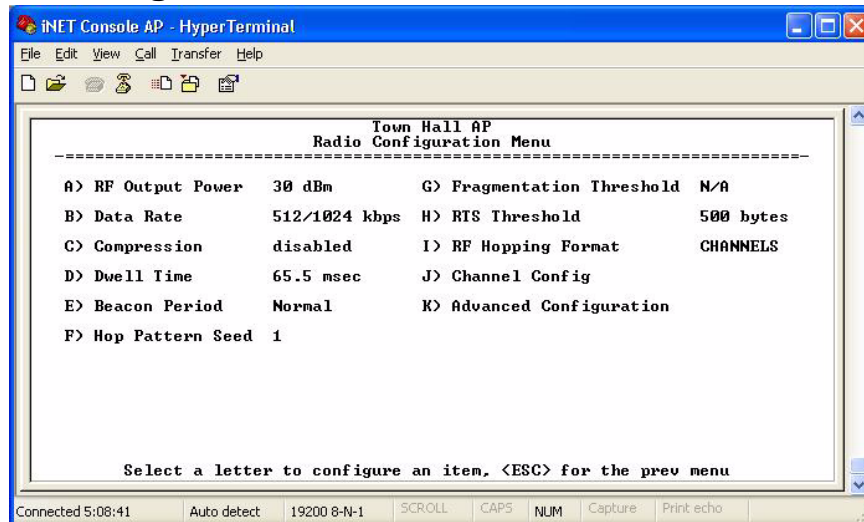


Figure 2-31. Radio Configuration Menu
(From iNET II Access Point Unit)

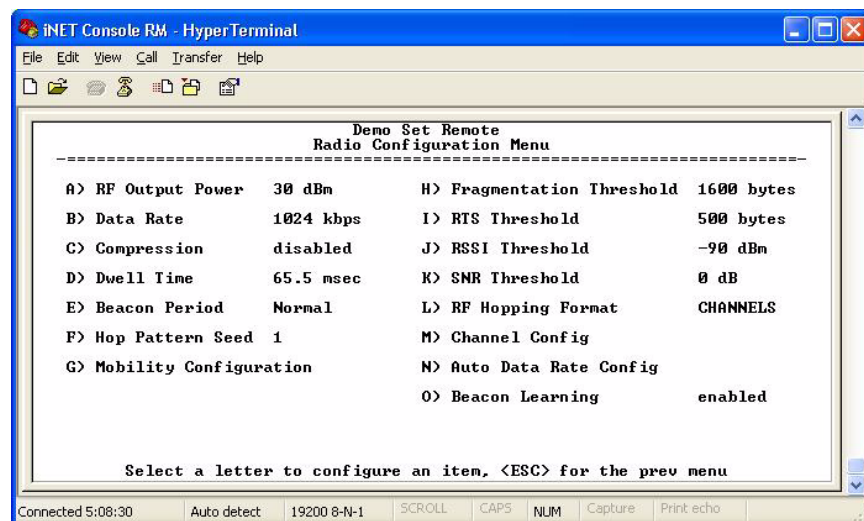


Figure 2-32. Radio Configuration Menu
(From iNET II Remote Unit)

- **RF Output Power**—Sets/displays RF power output level. Displayed in dBm. Setting should reflect local regulatory limitations and losses in antenna transmission line. (See “How Much Output Power Can be Used?” on Page 112 for information on how to calculate this value.)
[20–30; 20]

- **Data Rate** (*configurable on RM Only*)—Shows the over-the-air data rate setting for the Remote radio. Remotes can operate at one of two data rates when communicating with an AP: 1024 kbps (1 Mbps) or 512 kbps for iNET-II and 256 kbps or 512 kbps for iNET. The fastest data rate is possible with strong RF signal levels, typically stronger than -77 dBm RSSI including a 15 dB fade margin. When the data rate is set to **AUTO**, the remote radio is able to change speeds based on the signal quality criteria set in the Auto Data Rate submenu described later in this section (see Page 42).
[iNET: **256 kbps, 512 kbps, AUTO; 256 kbps**] [iNET-II: **512 kbps, 1024 kbps, AUTO; 512 kbps**]
- **Compression** (*configurable on AP Only*)—Enabling this option uses LZO compression algorithm for over-the-air data. Varying levels of data reduction are achieved depending on the nature of the information. Text files are typically the most compressible, whereas binary files are the least compressible. On average, a 30% increase in throughput can be achieved with compression enabled.
[**enabled, disabled; disabled**]
- **Dwell Time** (*configurable on AP Only*)—Duration (in milliseconds) of one hop on a particular frequency in the hopping pattern. Remotes get their value from AP upon association.
[iNET: **16.4, 32.8, 65.5, 131.1, 262.1; 65.5**]
[iNET-II: **16.4, 32.8, 65.5, 131.1; 65.5**]

TIP: If a packet is being transmitted and the dwell time expires, the packet will be completed before hopping to the next frequency.

- **Beacon Period** (*configurable on AP Only*)—Amount of time between Beacon transmissions (in msec).
Available Intervals for iNET: **Normal** (104 ms), **Fast** (52 ms), **Faster** (20 ms), **Slow** (508 ms), **Moderate** (208 ms). These values provide relatively quick association times where Fast is very fast (≈ 5 sec) and the other end, the largest recommended value, the 508 ms period is slow (≈ 60 sec). [**Normal, Fast, Faster, Slow, Moderate; Normal**]

For iNET II: **Normal** (52 ms), **Fast** (26 ms), **Faster** (10 ms), **Slow** (254 ms), **Moderate** (104 ms).

TIP: Increasing the Beacon Period will provide a *small improvement* in network data throughput. Shortening it decreases the time needed for Remotes to associate with the AP. A short beacon period is usually only a benefit when there are mobile Remotes in the network.

- **Hop Pattern Seed** (*configurable on AP Only*)—A user-selectable value to be added to the hop pattern formula. This is done in the unlikely event that identical hop patterns are used with two collocated or nearby networks. Changing the seed value will minimize the potential for RF-signal collisions in these situations. (This field is only changeable on an Access Point. Remotes read the AP's value upon association.) [**0 to 255; 1**]
- **Mobility Configuration** (*RM Only*)—This selection brings up a submenu where parameters related to mobile operation may be set. For details, See “**Mobility Configuration Menu**” on Page 47.
- **Fragmentation Threshold** (*configurable on RM Only*)—Before transmitting over the air, if a packet exceeds this number of bytes, the transceiver sends the packet in multiple fragments that are reassembled before being delivered over the Ethernet interface at the receiving end. Only even numbers are acceptable entries for this parameter. This option will only be configurable if Wireless Encryption is disabled. (See “Performance Notes” on Page 117 for additional information.) [**256–1600 bytes; 1600**]

TIP: In an interference-free environment this value should be large to maximize throughput. If interference exists then the value should be set to smaller values. The smaller the packet the less chance of it being interfered with at the cost of slightly reduced throughput.

NOTE: The radio does not support the simultaneous use of Fragmentation and Encryption. If encryption is enabled (other than RADIUS), the fragmentation option will not be available.

- **RTS Threshold**—Number of bytes for the over-the-air RTS/CTS handshake boundary. (See “Performance Notes” on Page 117.) [**0 to 1600 bytes; 500**]
-

NOTE: While the transceiver accepts RTS Threshold settings below 100, the lowest functioning value is 100.

TIP: Lower the **RTS Threshold** as the number of Remotes or overall over-the-air traffic increases. Using RTS/CTS is a trade-off, giving up some throughput in order to prevent collisions in a busy over-the-air network.

The **RTS Threshold** should be enabled and set with a value smaller than the **Fragmentation Threshold** described above. RTS forces the Remotes to request permission from the AP before sending a packet. The AP sends a CTS control packet to grant permission to one Remote. All other Remotes wait for the specified amount of time before transmitting.

- **RSSI Threshold (for alarm)**—Level (dBm) below which the received signal strength is deemed to have degraded, and a critical event (alarm) is generated and logged. Under these conditions, the PWR lamp flashes, and an SNMP trap is sent to the configured SNMP manager. [0 to -120; -90]
- **SNR Threshold (for alarm)**—Value (dB) below which the signal-to-noise ratio is deemed to have degraded and a critical event is generated and logged. Under these conditions, the PWR lamp flashes, and an SNMP trap is sent to the configured SNMP manager. [0 to 40; Not Programmed]
- **RF Hopping Format**—This option must be specified when the order is placed and cannot be modified in the field by the user. Operation must be compliant with country-specific restrictions. The available formats are:
 - **ISM:** 902–928 MHz band (iNET only)
 - **GSM:** 915–928 MHz band
 - **SPLIT:** 902-907.5 and 915-928 MHz bands
 - **CHANNELS:** 902–928 MHz, individual channels selectable within this range
- **Channel Config** (*Only applies to iNET-II, or specifically programmed iNETs*)—Brings up the submenu discussed in “Channel Config Menu” on Page 42.
- **Skip Zones** (*Only applies to iNET in ISM mode. Editable at AP Only.*)—This selection brings up a submenu discussed in “Advanced Configuration Menu” on Page 44.
- **Advanced Configuration** (*AP Only*)—Allows the user to control settings on the AP that are used during special circumstances. These parameters should not be modified unless specifically told to do so.
- **Auto Data Rate Configuration** (*Remote only*)—This selection brings up a submenu as shown in Figure 2-37. For the settings in this submenu to have any effect, the Data Rate menu item (Page 41) must be set to **AUTO**.
- **Beacon Learning (iNET-II Remote only)**—Gives the ability to configure the Remote for faster scanning and association. The Enabled option provides the standard iNET-II association behavior and is the default selection. When Beacon Learning is set to **on assoc**, the user must configure a subset of the AP’s channels on the Remote. This allows the Remote to scan the configured channels instead of the entire frequency band. The **Disabled** option requires the user to configure the Remote with the same channels as the AP. If the Remote’s configuration does not match, the Remote will not associate to the AP. [Enabled, Disabled, on assoc; Enabled]

2.5.2 Channel Config Menu

The Channel Configuration menu displays the utilization of channels in the 902–928 MHz range. This selection is available only on iNET-II or specially provisioned iNET units. The radio hops only on the channels selected in this menu.

NOTE: This menu changes when Beacon Learning is changed from **enabled** to **on assoc**. This applies to iNET-II radios only. See Figure 2-34 on Page 43.

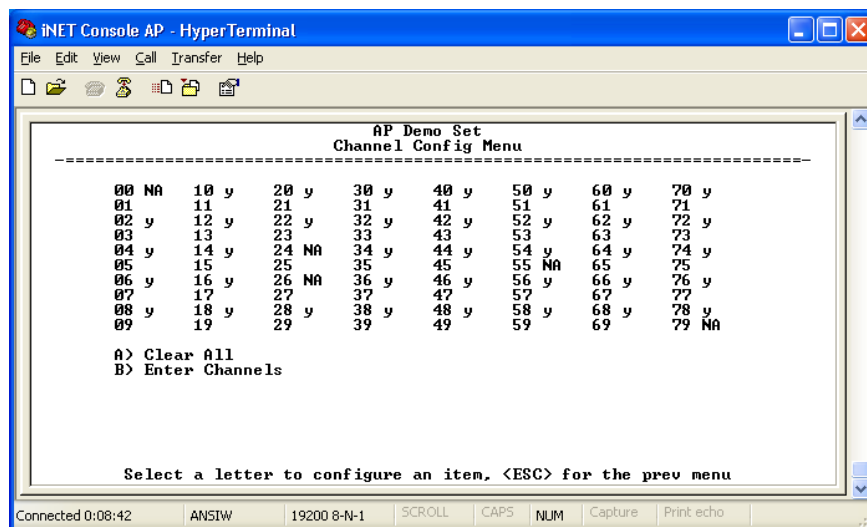


Figure 2-33. Channel Config Submenu

Key to channel indicators:

y (yes) = Radio channel is used

NA (not available) = Radio channel is not available

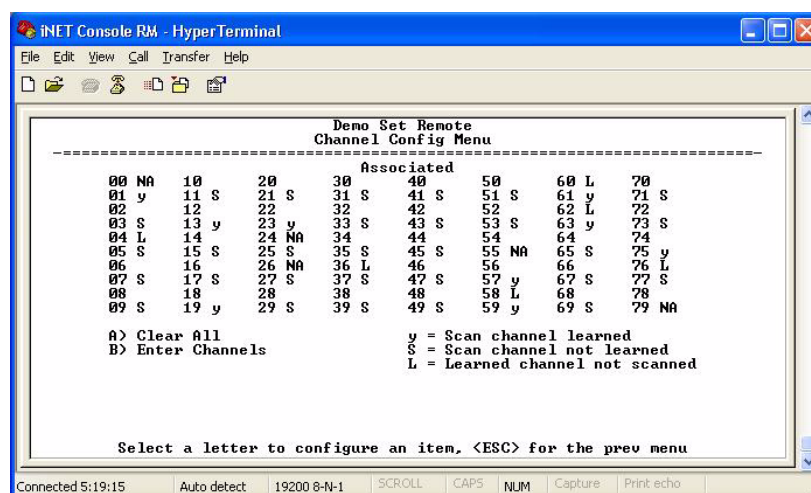


Figure 2-34. Channel Config Submenu using Beacon Learning

Key to channel indicators:

y = Configured channel learned from AP.

s = Configured channel was not in AP's channel configuration.

L = Channel that Remote did not scan for but learned from the AP on association.

NOTE: The options above are only configurable on the AP radio unless Beacon Learning on the Remote is set for **onassoc** or **disabled**. Remotes display this information as it is read from the AP.

- **Clear All**—This command clears all entries in the Channel Config Menu, resetting the available channels to “no usage.” Channels that are not available for use will appear with a notation of **NA**. These channels are not available because of pre-existing conditions, and are not user-configurable.
- **Enter Channels**—This allows selection of the channels used for frequency hopping operation. The selection of particular channels will result in an indication of **y**. Be aware that these channels do not become active until the **Commit Changes** selection is invoked.
- **Commit Changes**—Loads the active channels into the frequency list for frequency hopping operation.

2.5.3 Advanced Configuration Menu

Normally, the radio network is installed for an “always connected” mode of operation. The Advanced Configuration settings control radio behavior when your network is not running in this mode, such as when Mobility is enabled.

NOTE: These features should remain untouched unless instructed by GE MDS personal.

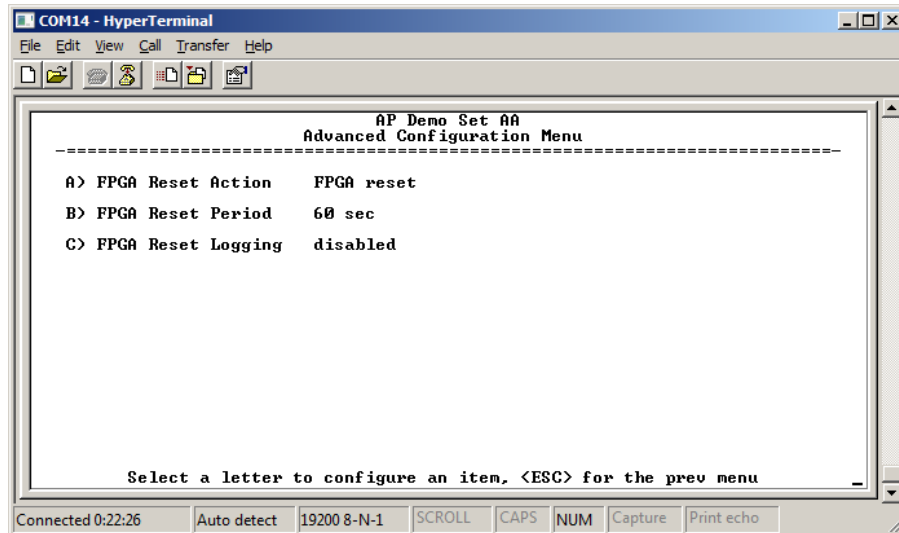


Figure 2-35. Advanced Configuration Submenu

- **FPGA Reset Action**—Action to take when the FPGA reset period expires. [**FPGA Reset, FPGA+MAC Reset, disabled; FPGA Reset**]
- **FPGA Reset Period**—Time interval (in seconds) to wait for a Remote before performing the FPGA reset action. [**10-600; 60**]
- **FPGA Reset Logging**—Control whether FPGA resets are logged in the event log. [**enabled, disabled; disabled**]

2.5.4 Skip Zones Menu

- **Skip Zones** (*Applies to iNET only. Editable at AP Only.*)—This selection brings up a submenu (Figure 2-36) that displays the current utilization of zones. Each zone consists of eight RF channels. In some instances there may be a part of the spectrum used by another system, that results in “continuous” or “persistent” interference to your system. To alleviate this form of interference, the transceiver may be programmed to “block out” affected portions of the spectrum using the Skip Zones Menu.

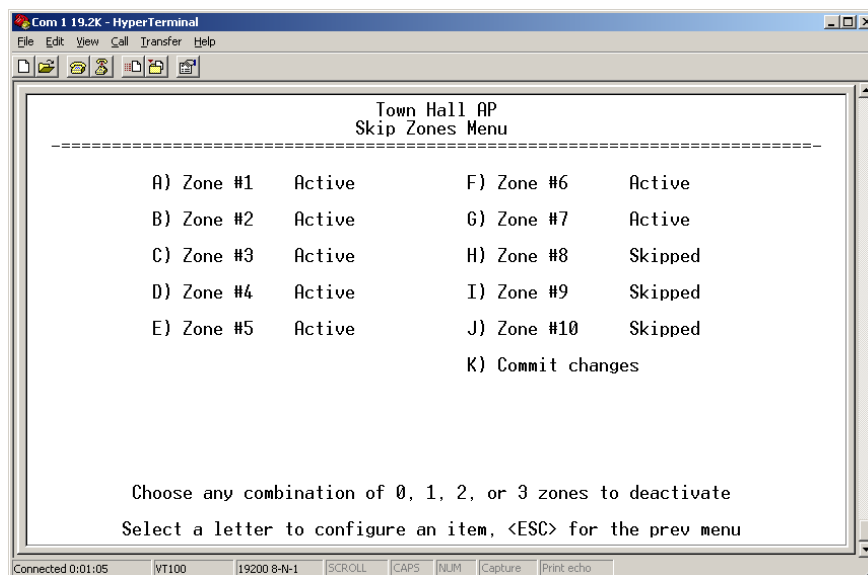


Figure 2-36. Skip Zone Options Submenu—MDS iNET Only
(“Commit changes” displayed only on Access Point radios)

Figure 2-36 displays the utilization of 10 zones, each having eight RF operating frequencies. Zones can be toggled between **Active** and **Skipped** at Access Points by first keying in the letter of the zone to be changed, then pressing the spacebar to toggle between the two options for each zone. Select **Commit Changes** to implement changes. These changes are forwarded to all units in the network through the AP’s beacon signal.

With an iNET radio (non-iNET-II), a maximum of three zones may be skipped to be compliant with FCC regulations.

2.5.5 Auto Data Rate Configuration Menu

The Auto Data Rate Configuration submenu is typically for use in environments where signal quality is variable, and you wish to maintain the highest possible over-the-air data rate as conditions change.

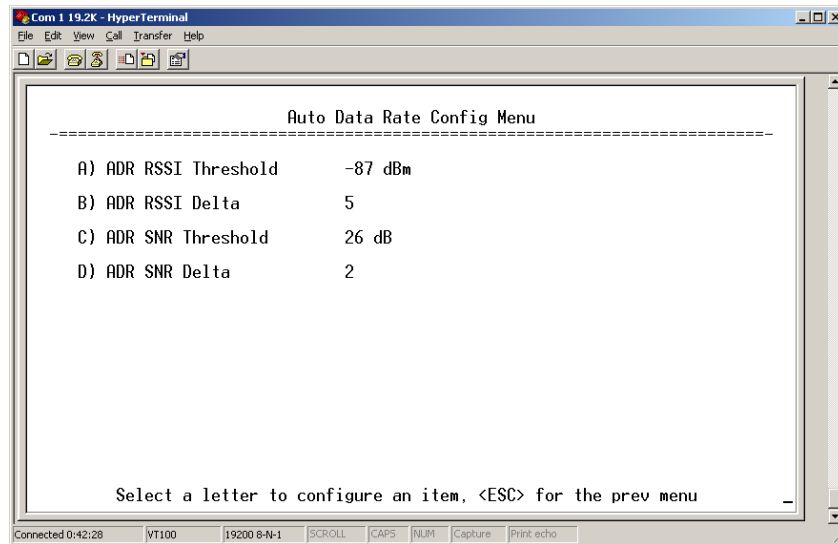


Figure 2-37. Auto Data Rate Submenu

- **ADR RSSI Threshold**—A specified received signal strength value, which, if exceeded by the range of the **RSSI Delta** setting, causes a data rate change in the transceiver. [-50 to -100; -87 dBm]
- **ADR RSSI Delta**—A user-specified *difference* from the **RSSI Threshold** figure which, if exceeded, causes a data rate change in the transceiver. [0-10; 5]
- **ADR SNR Threshold**—A user-specified signal-to-noise ratio, which, if exceeded by the range of the **SNR Delta** setting, causes a data rate change in the transceiver. [10-30; 26]
- **ADR SNR Delta**—A user-specified *difference* from the **SNR Threshold** figure which, if exceeded, causes a data rate change in the transceiver. [0-10; 2]

NOTE: In the following description, “high speed” refers to 512 kbps for the iNET radio and 1 Mbps for the iNET-II radio.

“Standard speed” refers to 256 kbps for the iNET radio and 512 kbps for the iNET-II.

Using the example of Figure 2-37, assume the current RSSI is -87 dBm. An RSSI reduction of more than 5 dBm (more negative RSSI number) would cause a data rate change from high speed to standard speed. Once the data speed has changed to standard speed, an RSSI *increase* to the level of -82 dBm would be required for the radio to switch back to high speed. This provides an operational “window” or hysteresis range over which the data speed stays constant despite minor changes in signal strength.

The SNR (signal-to-noise ratio) threshold and delta operate in the same manner described above, with the exception that the units are expressed in relative dB instead of dBm. In the example of Figure 2-37, a drop of 2 dB from a level of 26 dB would result in a data rate change from high speed to standard speed. For the radio to return to high speed, the SNR would need to increase to 28 dB. (*See Glossary for definition of SNR.*)

RSSI or SNR figures alone mean little when determining signal quality. Both parameters must be considered to get a true understanding of signal quality. For example, a strong, but noisy signal would likely be less useful than a weak signal with low noise levels. Proper use of the threshold and delta settings will result in smoother, more reliable performance from your wireless link.

Figure 2-37 shows the default values for RSSI and SNR parameters but these may be changed to optimize performance in your environment. In properly designed systems, experience has shown that RSSI levels between -50 dBm and -90 dBm provide reliable operation, provided the signal-to-noise ratio is 17 dB or above. Tailoring the thresholds with these baseline values in mind, can provide improved performance in your system.

NOTE: The RSSI is an average of the last 20 RSSI samples. The RSSI value is reset every time the radio returns to scanning mode.

2.5.6 Mobility Configuration Menu

A mobile environment requires special considerations that are not a factor in fixed installations. Use the following menu to set Remote radios for mobile operation.

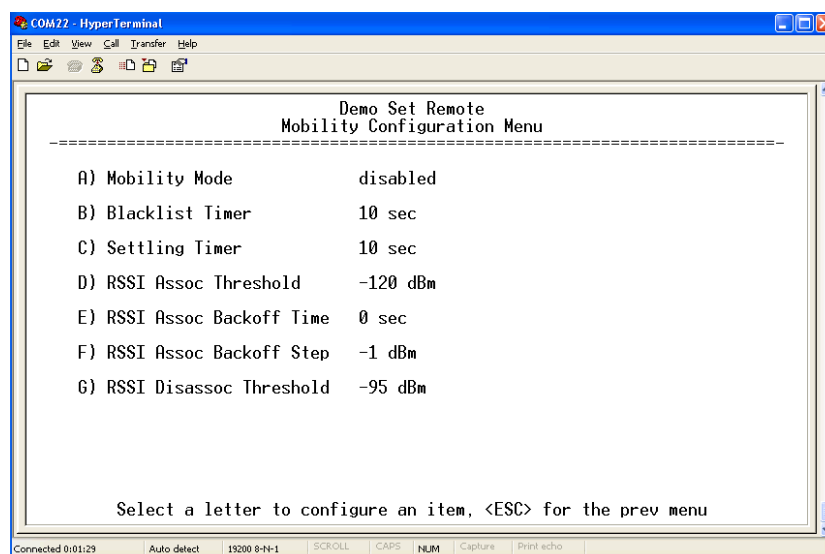


Figure 2-38. Mobility Configuration Menu (Remote only)

- **Mobility Mode**—Selects whether or not mobility-specific parameters are active. [enabled, disabled; disabled]
- **Blacklist Timer**—Sets/displays the number of seconds an AP stays on the blacklist after association is lost. [10-120; 10]
- **Settling Timer**—Sets/displays the number of seconds the radio waits before evaluating the signal quality of a newly acquired AP. [5-120; 10]
- **RSSI Assoc Threshold**—Level (dBm) that a Remote must read to determine whether or not to associate to an AP while in Mobility Mode. [0 to -120; -120]
- **RSSI Assoc Backoff Time**—Adjust the RSSI Assoc Threshold after scanning continues for this amount of time, repeating every specified number of seconds. A setting of 0 disables the feature. [0 – 120 seconds; 0]
- **RSSI Assoc Backoff Step**—Amount to adjust the RSSI Assoc Threshold at every backoff time. [-10 to -1 dBm; -1]
- **RSSI Disassoc Threshold**—Level (dBm) that a Remote will use to determine when to drop from its current AP if the signal becomes too degraded. [0 to -120; -90]

After association is lost with an AP, and scanning for an alternate AP is started, the former AP is placed on a “blacklist” to avoid linking immediately back to the same AP. Once the blacklist timer has expired, if no alternate AP is found, a link will be attempted with the same AP as before.

An Access Point is added to the blacklist when the Remote detects that the RSSI has dropped below the **RSSI Disassoc Threshold** and should try to find an alternate AP to connect to.

An Access Point is removed from the blacklist table when it has been in the table longer than the time set by the **Blacklist Timer**.

When mobility is enabled and beacon learning is on association, the dropped AP’s channels are excluded from scanning during the blacklist time.

Additional Considerations for Mobile Operation

The following key points should be considered for all mobile installations:

- Use middleware—The use of middleware in the mobile laptops is highly recommended for better operation of a mobile data system. GE MDS provides middleware from one of the vendors in this market. Contact your factory representative for details.
- Plan your network coverage—Deploy Access Points so that they provide overlapping coverage to each other. Access Points must use the same network name to enable roaming.
- Set the Remote radios to the lower speed (512 kbps for iNET-II, 256 kbps for iNET) to optimize coverage.
- Set the RSSI Threshold to -85 dBm—This level is typically used for mobile systems with good performance. Make sure there is overlapping coverage of more than one AP to provide a good user experience and continuous coverage.
- For the fastest scan/association time, change the Remotes' **Beacon Learning** from **enabled** to **on assoc** and set the channels to **scan** in "Channel Configuration Menu". This only applies to iNET-II Remotes running firmware 3.0.0 or newer.

At Every Mobile (Remote) Radio

- **Fragmentation Threshold [256]**—Set to a small value. This parameter defines the size of the message packets transmitted over the wireless media. These fragments are reconstructed into the original packet before delivery to the external device at the remote end of the link. In a mobile environment with rapidly changing conditions, setting this value to a minimum value improves the probability of packets being sent complete on the first try.

At Every AP Radio

Parameter settings that should be reviewed for AP radios providing service to mobile remotes:

- **Compression [disabled]**—Disable radio compression. Data compression is best performed by the middleware running on the mobile laptop PC. Gains in efficiency are made because middleware compresses data at a higher stack level, and it aggregates multiple data frames and streams into a single packet. Compression at the radio level, although highly efficient, works at the individual packet level.
- **Dwell Time [Set to the minimum value]**—This setting controls the amount of time that the unit spends on each frequency between hops. Although overall throughput appears to decrease by this setting the effects of multipath fading are minimized through frequency diversity.
- **Beacon Period [Set to the fastest value]**—This parameter defines the interval at which the Access Point transmits a synchronization beacon to all remotes. A faster setting minimizes resynchronization times when remote radios roam between access points or in highly interrupted coverage areas (dense buildings, for example).
- **RTS Threshold [0 -1600 bytes]**—Enable RTS flow at a small value. This setting is a wireless equivalent to RTS/CTS flow control in a wired communications circuit. This mechanism prevents packet collisions caused by the "Hidden Node" scenario, in which remotes can't hear each other before transmitting. When this value is set below 100 or above 1500, it is effectively disabled.
- **Spanning Tree Protocol [enabled/disabled]**—This setting controls the enabling and disabling of Spanning Tree Protocol (STP). STP is used to prevent loops from being created when connecting bridges in parallel.

2.6 Configuring the Serial Ports

2.6.1 Overview

The transceiver includes an embedded serial device server that provides transparent encapsulation over IP. In this capacity, it acts as a gateway between serial and IP remote devices. Two common scenarios are PC applications using IP to talk to remote devices, and serial PC applications talking to remote serial devices over an IP network.

Essentially the same data services are available for both serial ports: COM1 and COM2. Note that the transceiver's COM1 port is DCE and COM2 is DTE. Therefore, if the RTU to be connected is also DTE, then a null-modem cable will need to be used when connecting to COM2.

NOTE: In the discussion that follows, COM1 and COM2 will be treated alike unless noted.

Com1 Port—Dual Purpose Capability

The COM1 port is used as a local console connection point and to pass serial data with an external device. Setting the COM1 port status to **Enable** prevents access to the Management System (MS) through this port. However, the MS can still be accessed via the LAN port using Telnet or a web browser.

To restore the COM1 port to support Management System services, connect a terminal to the port, select the proper baud rate (19,200 is default), and enter an escape sequence (+++) to reset it to the console mode.

TCP vs. UDP

Both types of IP services are used by the transceiver embedded serial device server—TCP and UDP. TCP provides a connection-oriented link with end-to-end acknowledgment of data, but with some added overhead. UDP provides a connectionless best-effort delivery service with no acknowledgment.

Most polled protocols will be best served by UDP service as the protocol itself has built-in error recovery mechanisms. UDP provides the needed multidrop operation by means of multicast addressing.

On the other hand, TCP services are best suited for applications that do not have a recovery mechanism (error-correction) and must have the guaranteed delivery that TCP provides despite the extra overhead. The IP-to-Serial example shows how to do this. (See “Configuring for DF1/EIP” on Page 57.)

Serial Encapsulation

Transparent encapsulation, or IP tunneling, provides a mechanism to encapsulate serial data into an IP envelope. Basically, all the bytes received through the serial port are put into the data portion of a TCP or UDP packet (TCP or UDP are user configurable options). In the same manner, all data bytes received in a TCP or UDP packet are output through the serial port.

When data is received by the radio through the serial port it is buffered until the packet is received completely. There are two events that signal an end-of-packet to the radio: a period of time since the last byte was received, or a number of bytes that exceed the buffer size. Both of these triggers are user configurable.

One radio can perform serial data encapsulation (IP-to-Serial) and talk to a PC. Two radios (or one radio and a terminal server) can be used together to provide a serial-to-serial channel.

TCP Client vs. TCP Server

A TCP session has a server side and a client side. You can configure the transceiver to act as a server, a client, or both.

TCP servers listen and wait for requests from remote TCP clients to establish a session. A TCP client is a program running on a device other than the TCP server. Alternately, TCP clients actively attempt to establish a connection with a TCP server. In the case of the transceiver, this happens whenever data is received on the serial port.

When the unit is configured as both TCP Client and Server, the transceiver will operate in either client or server mode, depending on which event occurs first, either receiving data on the serial port, or receiving a request to open a TCP connection from a remote client.

The transceiver keeps a TCP session open until internal timers that monitor traffic expire. Once a TCP session is closed, it must be opened again before traffic can flow.

UDP Multicast

IP provides a mechanism to do a limited broadcast to a specific group of devices. This is known as “multicast addressing.” Many IP routers, hubs and switches support this functionality.

Multicast addressing requires the use of a specific branch of IP addresses set apart by the Internet Assigned Numbers Authority (IANA) for this purpose.

UDP multicast is generally used to transport polling protocols typically used in SCADA applications where multiple remote devices will receive and process the same poll message.

As part of the Multicast implementation, the radio sends IGMP membership reports and IGMP queries, and responds to membership queries. It defaults to V2 membership reports, but responds to both V1 and V2 queries.

You must configure the multicasted serial port as the target for the multicast data (for example, multi-point-to-multipoint mode, or point-to-multipoint mode where the inbound data is multicast). This restriction is because a host that only sends data to a multicast address (for example, point-to-multipoint mode where the iNET acts as a point) will not join the group to receive multicast data because the host’s inbound data is directed unicast data.

The serial-to-serial example which follows shows how to provide multicast services. (See “Point-to-Multipoint IP-to-Serial Application Example” on Page 59.)

PPP

External devices can connect to the transceiver using PPP (Point-to-Point Protocol). The transceiver works as a server and assigns an IP address to the device that connects through this interface.

To gain access to the transceiver from a PC even if the network is down, a modem may be connected to one of the transceiver’s COM ports that has been configured with PPP.

DF1/EIP

NOTE: DF1/EIP is only supported on MDS iNET 900 ENI and MDS iNET-II 900 radios. Refer to your product to determine the radio’s capabilities.

The MDS iNET/ENI embeds the Ethernet/IP networking functionality of Rockwell’s ENI adapter into the iNET 900 transceiver. With some minor exceptions, the iNET/ENI duplicates the functionality of the 1761-NET-ENI, providing Ethernet/IP connectivity to any device using the full-duplex DF1 protocol. More information can be found in Appendix A, *MDS iNET/ENI Protocols* (beginning on Page 132).

MODBUS/TCP

NOTE: MODBUS/TCP is only supported on MDS iNET 900 ENI and MDS iNET-II 900 radios. Refer to your product to determine the radio’s capabilities.

The transceiver implements a MODBUS/TCP server that bridges MODBUS/TCP to either **Modbus RTU** or **Modbus/ASCII**. It does *not* function as a MODBUS/TCP client.

The transceiver converts MODBUS/TCP requests to either RTU or ASCII serial MODBUS packets and sends them to the configured serial port. The transceiver waits up to the timeout period for a reply on the serial port, and if a reply arrives, the transceiver converts the response back to MODBUS/TCP and sends it to the connected MODBUS/TCP client. More information can be found in Appendix A, *MDS iNET/ENI Protocols* (beginning on Page 132).

NOTE: MODBUS is possible on the COM2 port only.

NOTE: For information on the MDS iNET 900 ENI, which provides expanded gateway and protocol conversion capabilities not found in the iNET 900 (DF1 to EIP, and MODBUS to MODBUS TCP conversions), refer to Appendix A, *MDS iNET/ENI Protocols* (beginning on Page 132).

Data Buffering

Data buffering is always active regardless of the selected mode. When Seamless mode is selected, a buffer size of 256 bytes is used. When custom mode is selected, the size options are: 16, 32, 64, 128, and 256 bytes. The Inter-Frame Delay is settable in either Seamless or Custom modes.

Implementing Configuration Changes

There are several configuration parameters for the Serial Gateway found under the *Serial Configuration Menu* of the Management System. After making changes to the configuration, you must use the menu's "Commit Changes" to assert the changes.

If you are connecting EIA-232 serial devices to the transceiver, review these parameters carefully.

Serial Configuration Wizard

The Serial Configuration Wizard available through the **Serial Gateway Configuration Menu** is recommended for configuration of serial ports. The wizard uses a step-by-step process, will eliminate possible conflicting settings, and streamline complex configurations.

The wizard can be bypassed by selecting option **B) View Current Settings** and adjusting the individual settings of the appropriate parameter.

2.6.2 Serial Data Port Configuration Menu

The first two menu items present the identical parameter fields for each port with one exception—Flow Control. This is available only on COM2.

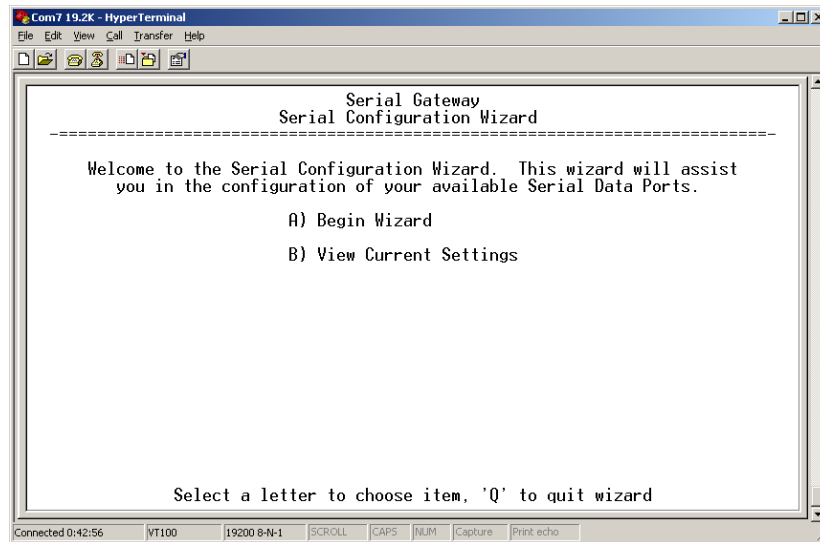


Figure 2-39. Serial Configuration Wizard

- **Begin Wizard**—Tool for configuration of serial ports using a step-by-step process.
- **View Current Settings**—Displays all settable options, depending on the selected IP protocol.

2.6.3 Configuring for UDP Mode

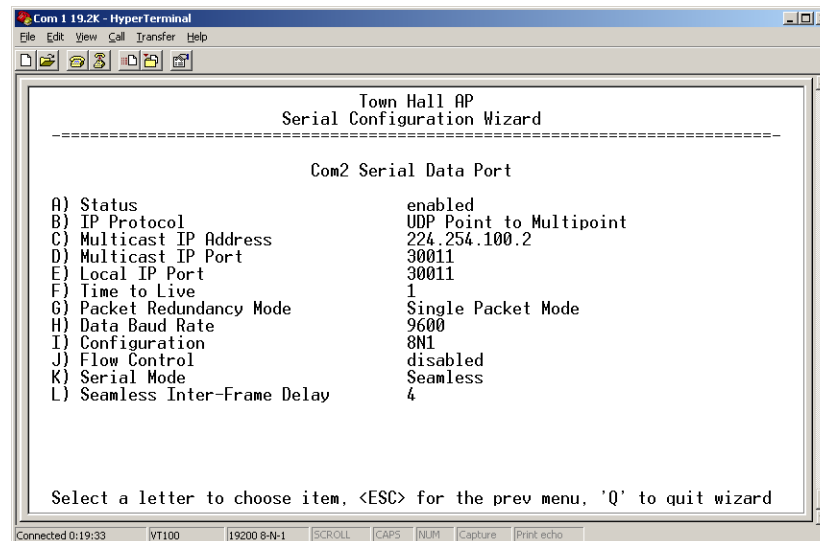


Figure 2-40. UDP Point-to-Multipoint Menu

Use UDP point-to-multipoint to send a copy of the same packet to multiple destinations, such as in a polling protocol.

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—Point to Multipoint [TCP, UDP PPP, DF1/EIP, MODBUS/TCP Server; TCP]. This is the type of IP port that will be offered by the transceiver's serial device server.
- **Multicast IP Address** (used instead of **Local IP Address** when using UDP Point-to-Multipoint.)—Must be configured with a valid Class D IP address (224.0.0.0–239.255.255.255). IP packets received with a matching destination address will be processed by this unit [**Any valid IP address; 0.0.0.0**].

- **Multicast IP Port** (used instead of **Local IP Port** when using UDP Point-to-Multipoint.)—This port number must match the number used by the application connecting to local TCP or UDP socket. [1-64,000; **COM1: 30010, COM2: 30011**]
- **Local IP Port**—Receive IP data from this source and pass it through to the connected serial device. The port number must be used by the application connecting to local TCP or UDP socket. [Any valid IP port; **COM1: 30010, COM2: 30011**]
- **Time to Live (TTL)**—An IP parameter defining the number of hops that the packet is allowed to traverse. Every router in the path will decrement this counter by one. [1-255 hops; 1]
- **Packet Redundancy Mode**—For proper operation, all radios' Serial Packet Redundancy mode must match (Single Packet mode vs. Packet Repeat mode). This is because a transceiver, when in Packet Repeat mode, sends 12 extra characters (sequence numbers, etc.) to control the delivery of the repeated data. Misconfigurations can result in undesired operation.
- **Data Baud Rate**—Data rate (payload) for the COM port in bits-per-second. [1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200; 19200]
- **Configuration**—Formatting of data bytes, representing data bits, parity and stop bits. [7N1, 7E1, 7O1, 8N1, 8E1, 8O1, 7N2, 7E2, 7O2, 8N2, 8E2, 8O2; 8N1]
- **Flow Control (Com2 Only)**—RTS/CTS handshaking between the transceiver and the connected device. [Enabled, Disabled; Disabled]
- **Serial Mode**—When seamless mode is selected data bytes entering the serial data port are sent over the radio link without delay, but the receiving end will buffer the data until enough bytes have arrived to cover worst-case gaps in transmission. The delay introduced by data buffering may range from 22 to 44 ms, but the radio will not create any gaps in the *output* data stream. This permits operation with protocols such as MODBUS™ that do not allow gaps in their data transmission. [Seamless, Custom; Seamless]
- **Seamless Inter-Frame Delay**—Amount of time (in number of characters) that signal the end of a message (inter-character time-out). UDP packet sizes are delimited and sent out based on the Seamless Inter-Frame Delay only when receiving data through the serial port. MODBUS defines a “3.5-character” setting. [1-65,535; 4]

TIP: To convert this delay into milliseconds, multiply the number of characters configured here by 10 (there are usually 10 bits in each byte) and divide the result by the data rate of the serial port (in kbps).

- **Custom Data Buffer Size** (Custom Packet Mode only)—Maximum amount of characters that the Remote end will buffer locally before starting to transmit data through the serial port. [16, 32, 64, 128, 256; 32]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

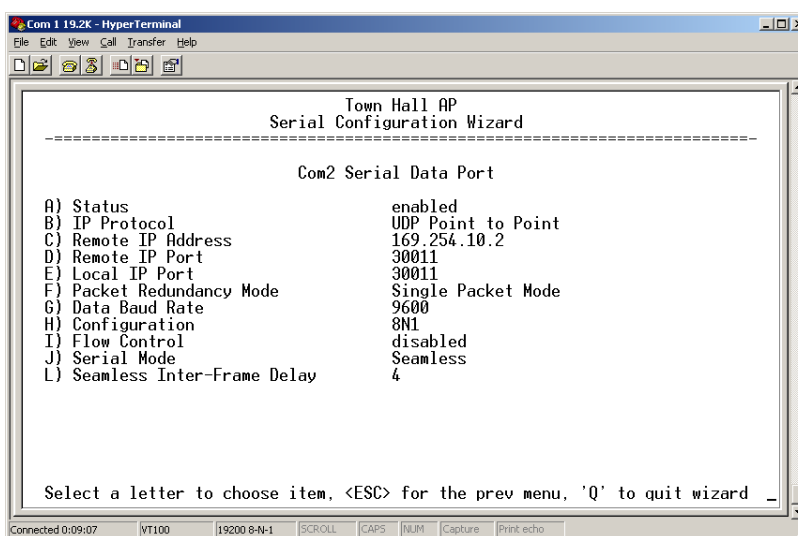


Figure 2-41. UDP Point-to-Point Menu

Use UDP point-to-point configuration to send information to a single device.

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—UDP Point-to-Point. This is the type of IP port that will be offered by the transceiver's serial device server. [TCP, UDP, PPP, DF1/EIP, MODBUS/TCP Server; TCP]
- **Remote IP Address**—Data received through the serial port is sent to this IP address. To reach multiple Remotes in the network, use UDP Point-to-Multipoint. [Any valid IP address; 0.0.0.0]
- **Remote IP Port**—The destination IP port for data packets received through the serial port on the transceiver. [1–64,000; Default COM1: 30010, Default COM2: 30011]
- **Local IP Port**—Port number where data is received and passed through to the serial port. This port number must be used by the application connecting to this transceiver. [1–64,000; COM1: 30010, COM2: 30011]
- **Packet Redundancy Mode**— For proper operation, all radios' Serial Packet Redundancy mode must match (Single Packet mode vs. Packet Repeat mode). This is because a transceiver, when in Packet Repeat mode, sends 12 extra characters (sequence numbers, etc.) to control the delivery of the repeated data. Misconfigurations can result in undesired operation.
- **Data Baud Rate**—Data rate (payload) for the COM port in bits-per-second. [1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200; 19200]
- **Configuration**—Formatting of data bytes. Data bits, parity and stop bits [7N1, 7E1, 7O1, 8N1, 8E1, 8O1, 7N2, 7E2, 7O2, 8N2, 8E2, 8O2; 8N1].
- **Flow Control (COM2 only)**—RTS/CTS handshaking between the transceiver and the connected device. [Enabled, Disabled; Disabled]
- **Serial Mode**— When seamless mode is selected, data bytes will be sent over the air as quickly as possible, but the receiver will buffer the data until enough bytes have arrived to cover worst case gaps in transmission. The delay introduced by data buffering may range from 22 to 44 ms, but the radio will not create any gaps in the output data stream. This mode of operation is required for protocols such as MODBUS™ that do not allow gaps in their data transmission. [Seamless, Custom; Seamless]
- **Seamless Inter-Frame Delay**— Number of characters that represent the end of a message (inter-character time-out). MODBUS defines a “3.5-character” parameter. [1–65,535; 4]
- **Custom Data Buffer Size (Custom Packet Mode only)**—Maximum amount of characters that the Remote end will buffer locally before starting to transmit data through the serial port. [16, 32, 64, 128, 256; 32]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

2.6.4 Configuring for TCP Mode

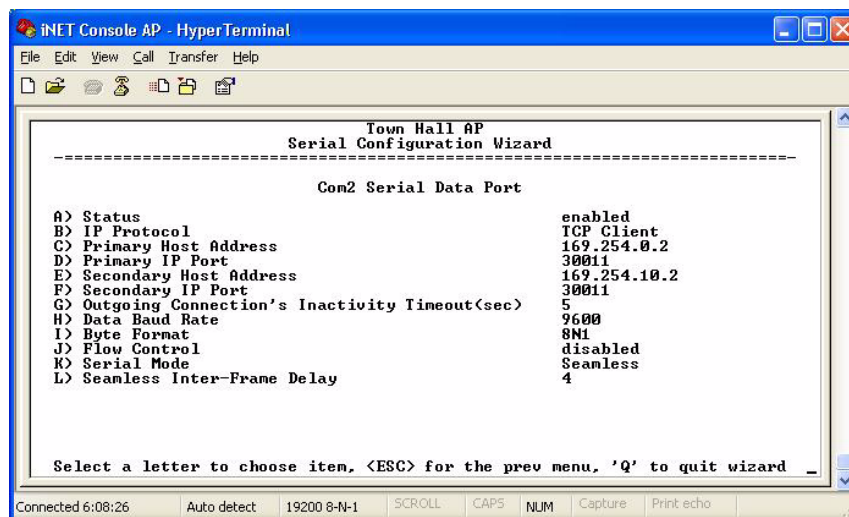


Figure 2-42. TCP Client Menu (Remote)

- **Status**—Enable/Disable the serial data port.

- **IP Protocol**—TCP Client. This is the type of IP port that will be offered by the transceiver's serial device server. [TCP, UDP, PPP, DF1/EIP, MODBUS/TCP Server; TCP]
- **Primary Host Address**—The IP address to be used as a destination for data received through the serial port. [Any valid IP address; 0.0.0.0]
- **Primary IP Port**—The destination IP port for data packets received through the serial port on the transceiver. [Any valid IP port; Default COM1: 30010, Default COM2: 30011]
- **Secondary Host Address**—The IP address to be used as a destination for data received through the serial port in case the primary host address is not available. [Any valid IP address; 0.0.0.0]
- **Secondary IP Port**—The destination IP port for data packets received through the serial port on the transceiver used along with the secondary host address above. [Any valid IP port; Default COM1: 30010, Default COM2: 30011]
- **Outgoing Connection's Inactivity Timeout (sec)**—Amount of time (in seconds) that the transceiver will wait for data before terminating the TCP session. [0–600; 600]
- **Data Baud Rate**—Data rate (payload) for the COM port in bits-per-second. [1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200; 19200]
- **Byte Format**—Interface signaling parameters. Data bits, parity and stop bits. [7N1, 7E1, 7O1, 8N1, 8E1, 8O1, 7N2, 7E2, 7O2, 8N2, 8E2, 8O2; 8N1]
- **Flow Control (Com2 Only)**—RTS/CTS handshaking between the transceiver and the connected device. [Enabled, Disabled; Disabled]
- **Serial Mode**— If data buffering is Enabled, the radio will operate in seamless mode. Data bytes will be sent over the air as quickly as possible, but the receiver will buffer the data until enough bytes have arrived to cover worst case gaps in transmission. The delay introduced by data buffering may range from 22 to 44 ms, but the radio will not create any gaps in the output data stream. This mode of operation is required for protocols such as MODBUS™ and some variants which do not allow gaps in their data transmission. [Seamless, Custom; Seamless]
- **Seamless Inter-Frame Delay**— Number of characters that represent the end of a message (inter-character time-out). MODBUS defines a “3.5-character” parameter. [1–65,535; 4]
- **Custom Data Buffer Size (Custom Packet Mode only)**—Maximum amount of characters that the Remote end will buffer locally before starting to transmit data through the serial port. [16, 32, 64, 128, 256; 32]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

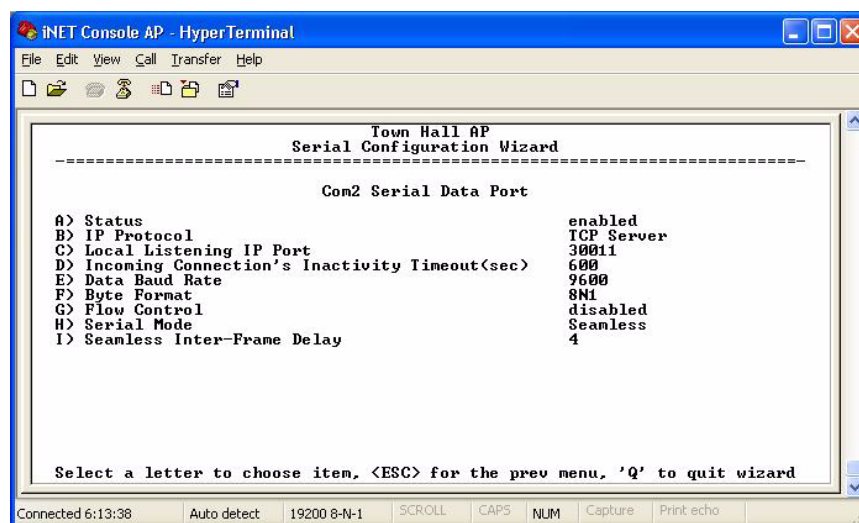


Figure 2-43. TCP Server Menu (AP)

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—TCP Server. This is the type of IP port that will be offered by the transceiver's serial device server. [TCP, UDP, PPP, DF1/EIP, MODBUS/TCP Server; TCP]

- **Local Listening IP Port**—Receive IP data from this source and pass it through to the connected serial device. The port number must be used by the application connecting to local TCP or UDP socket. [Any valid IP port; **Default COM1: 30010, Default COM2: 30011**]
- **Incoming Connections Inactivity Timeout (sec)**—Amount of time (in seconds) that the receiver listens for connections before resetting.
- **Data Baud Rate**—Data rate (payload) for the COM port in bits-per-second. [1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200; 19200]
- **Byte Format**—Interface signaling parameters. Data bits, parity and stop bits. [7N1, 7E1, 7O1, 8N1, 8E1, 8O1, 7N2, 7E2, 7O2, 8N2, 8E2, 8O2; 8N1].
- **Flow Control (COM2 only)**—RTS/CTS handshaking between the transceiver and the connected device. [Enabled, Disabled; Disabled]
- **Serial Mode**— If data buffering is Enabled, the radio will operate in seamless mode. Data bytes will be sent over the air as quickly as possible, but the receiver will buffer the data until enough bytes have arrived to cover worst case gaps in transmission. The delay introduced by data buffering may range from 22 to 44 ms, but the radio will not create any gaps in the output data stream. This mode of operation is required for protocols such as MODBUS™ and some variants which do not allow gaps in their data transmission. [Seamless, Custom; Seamless]
- **Seamless Inter-Frame Delay**— Number of characters that represent the end of a message (inter-character time-out). MODBUS defines a “3.5-character” parameter. [1–65,535; 4]
- **Custom Data Buffer Size** (Custom Packet Mode only)—Maximum amount of characters that the Remote end will buffer locally before starting to transmit data through the serial port. [16, 32, 64, 128, 256; 32]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

2.6.5 Configuring for PPP Mode

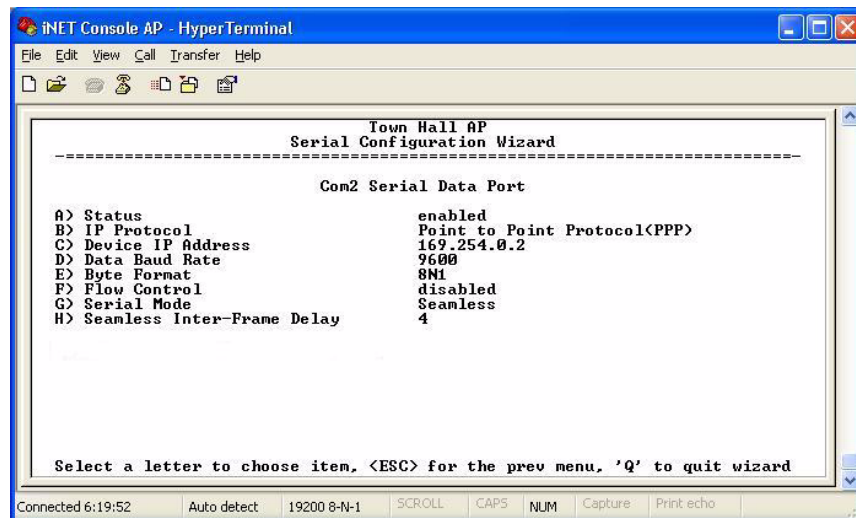


Figure 2-44. PPP Menu

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—PPP. This is the type of IP port that will be offered by the transceiver’s serial device server. [TCP, UDP, PPP, DF1/EIP, MODBUS/TCP Server; TCP]
- **Device IP Address**—IP address that will be assigned to the dialing device once the connection is established. [0.0.0.0]
- **Data Baud**—The baud rate of the serial port of the transceiver to which the external device is connected. [1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200; 19200]
- **Byte Format**—Byte format of the serial port. [7N1, 7E1, 7O1, 7N2, 7E2, 7O2, 8N1, 8E1, 8O1, 8N2, 8E2, 8O2; 8N1]
- **Flow Control (COM2 only)**—RTS/CTS handshaking between the transceiver and the connected device. [Enabled, Disabled; Disabled]

- **Serial Mode**—When seamless mode is selected, data bytes will be sent over the air as quickly as possible, but the receiver will buffer the data until enough bytes have arrived to cover worst case gaps in transmission. The delay introduced by data buffering may range from 22 to 44 ms, but the radio will not create any gaps in the output data stream. This mode of operation is required for protocols such as MODBUS™ that do not allow gaps in their data transmission. [Seamless, Custom; Seamless]
- **Seamless Inter-Frame Delay**— Number of characters that represent the end of a message (inter-character time-out). MODBUS defines a “3.5-character” parameter. [1–65,535; 4]

NOTE: With MODBUS/RTU mode, poll requests may be fragmented when using COM port baud rates above 19200 bps via a USB/Serial adapter (FTDI). This may cause incorrect checksum/CRC errors and thus, timeouts.

- **Custom Data Buffer Size** (Custom Packet Mode only)—Maximum amount of characters, that the Remote end will buffer locally before starting to transmit data through the serial port. [16, 32, 64, 128, 256; 32]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

A PPP session shows the following possible states:

- **Sending LCP Requests**—The PPP server is querying for any clients that need to connect.
- **Link Established**—A successful PPP connection has been negotiated and an IP address is assigned.
- **Port not Enabled**—The serial port is disabled.

2.6.6 Configuring for DF1/EIP

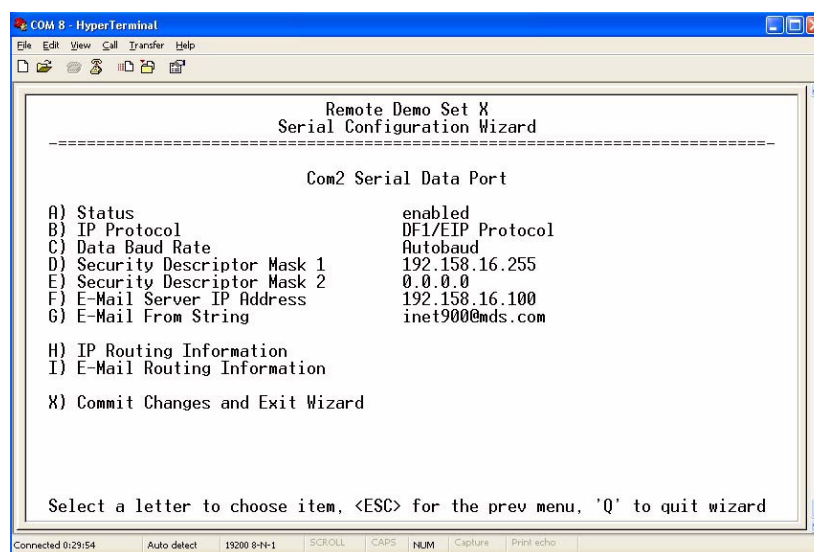


Figure 2-45. DF1/EIP Protocol Menu

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—DF1/EIP Protocol. This is the type of IP port that will be offered by the transceiver’s serial device server. [TCP, UDP, PPP, DF1/EIP, MODBUS/TCP Server; TCP]
- **Data Baud Rate**—The baud rate of the transceiver’s serial port to which the external device is connected. [1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, Autobaud; Autobaud]
- **Security Descriptor Mask 1/2**—Use to control which IP addresses can access the serial device connected to the iNET radio. [Valid IP Address; 0.0.0.0]
- **Email Server IP Address**—IP Address of the (optional) email server. [Valid IP Address; 0.0.0.0]
- **Email From String**—Text to identify the sender. [Valid email address; blank]
- **IP Routing Information**—The desired IP addresses for message routing.
- **Email Routing Information**—The desired email destination address(es) for message routing.

2.6.7 Configuring for MODBUS/TCP Server

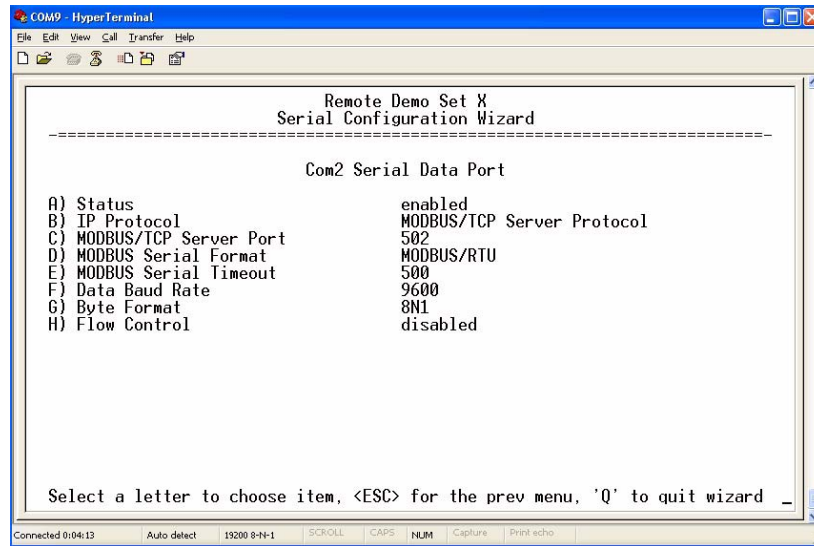


Figure 2-46. MODBUS/TCP Server Menu

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—MODBUS/TCP Server. This is the type of IP port that will be offered by the transceiver's serial device server. **[TCP, UDP, PPP, DF1/EIP, MODBUS/TCP Server; TCP]**
- **MODBUS/TCP Server Port**—Port on which the MODBUS/TCP Server will listen. **[0-65535; 502]**
- **MODBUS Serial Format**—The desired MODBUS Serial format **[MODBUS/RTU, MODBUS/ASCII; MODBUS/RTU]**

NOTE: The only difference between MODBUS/RTU and MODBUS/ASCII is the form of the framing sequence, error check pattern, and address interpretation.

- **MODBUS Serial Timeout**—MODBUS serial timeout in milliseconds (ms). **[100-65535; 500]**
 - **Data Baud Rate**—The baud rate of the transceiver's serial port to which the external device is connected. **[1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200; 9600]**
 - **Byte Format**—Byte format of the serial port. **[7N1, 7E1, 701, 7N2, 7E2, 702, 8N1, 8E1, 801, 8N2, 8E2, 802; 7N1]**
 - **Flow Control**—RTS/CTS handshaking between the transceiver and the connected device. **[Enabled, Disabled; Disabled]**
-

NOTE: MODBUS/TCP functionality is provided on the COM2 port only.

2.6.8 IP-to-Serial Application Example

You have a choice to use UDP or TCP to establish communications. This will depend on the type of device you are communicating with at the other end of the IP network. TCP is illustrated in this example.

In TCP mode, the transceiver remains in a passive mode offering a socket for connection. Once a request is received, data received at the serial port will be sent out through the IP socket and vice versa, until the connection is closed, or the link is interrupted. In this mode, the transceiver behaves the same, whether it is an Access Point or a Remote (refer to Figure 2-47 and Table 2-1 on Page 59).

NOTE: The TCP session has a timeout of 10 minutes (600 seconds). If inactive for that time, it will be closed. The transceiver will offer the port again for connection after this time expires.

Establishing a Connection

From the PC, establish a TCP connection to the IP address of the Remote transceiver and to the IP port as configured in Table 2-1 (30010—COM1, 30011—COM2). A Telnet client application can be used to establish this connection. Data can now be sent between the PC and the RTU or other connected device.

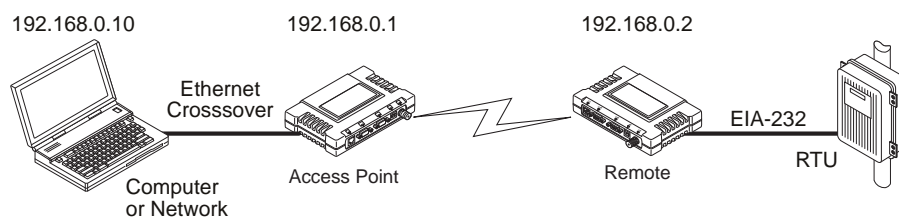


Figure 2-47. IP-to-Serial Application Diagram

Table 2-1. Serial Port Application Configuration
(IP-to-Serial Connection)

Transceiver Location	Menu Item	Setting
Access Point	None is required	None is required
Remote Unit	IP Address	192.168.0.2
	Status	Enabled
	IP Protocol	TCP
	Baud Rate	9,600 (Example)
	Flow Control	None
	Local IP Port	30011

2.6.9 Point-to-Multipoint IP-to-Serial Application Example

The operation and data flow for this mode is very similar to Point-to-Point serial-to-serial application, except that it uses multicast addressing. The primary difference is that the PC uses UDP to communicate with all of the Remotes. Upon receiving the packet, each Remote strips the data out of the UDP packet and sends it from its COM port. Likewise, data presented at any of the Remotes' COM ports is packetized, sent to the PC using the Access Point (see Figure 2-48 and Table 2-2 on Page 60).

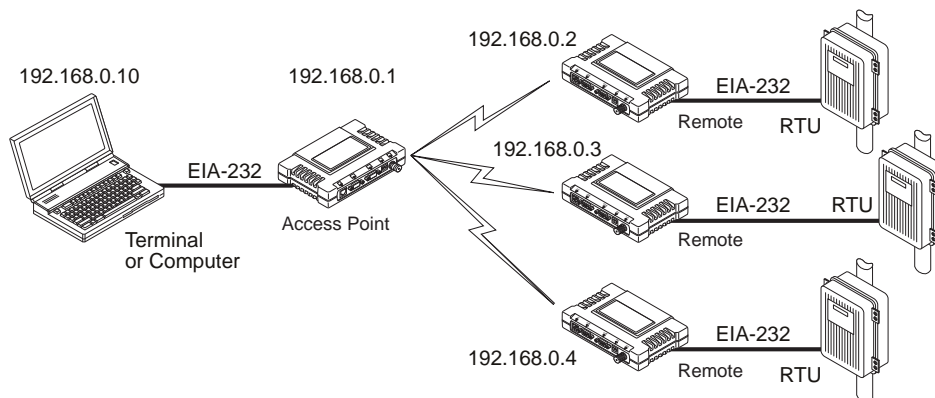


Figure 2-48. Point-to-Multipoint IP-to-Serial Application Diagram

Table 2-2. Serial Port Application Configuration

Transceiver Location	Menu Item	Setting
PC	IP Protocol	UDP
	Remote IP Address	224.254.1.1— Multicast Address ¹
	Local IP Port	30011
Access Point (COM2) ²	N/A	None required
Remote Units (COM2) ²	Enable	Enabled
	Baud Rate	2,400 (Example)
	Serial Mode	Custom
	Flow Control ³	Hardware (Example)
	IP Protocol	UDP
	Remote IP Address	192.168.0.1
	Remote IP Port	30011
	Local IP Port	30011
	Local Multicast Address	224.254.1.1 — Multicast Address ¹

1. This address is an example only. Any Class D IP address (224.0.0.0–239.255.255.255) will work.
2. Either COM port can be used, but they must be the same ones at both ends of the link. Both COM ports can be used simultaneously for two independent data channels.
3. Flow Control applies to the COM2 Port only.

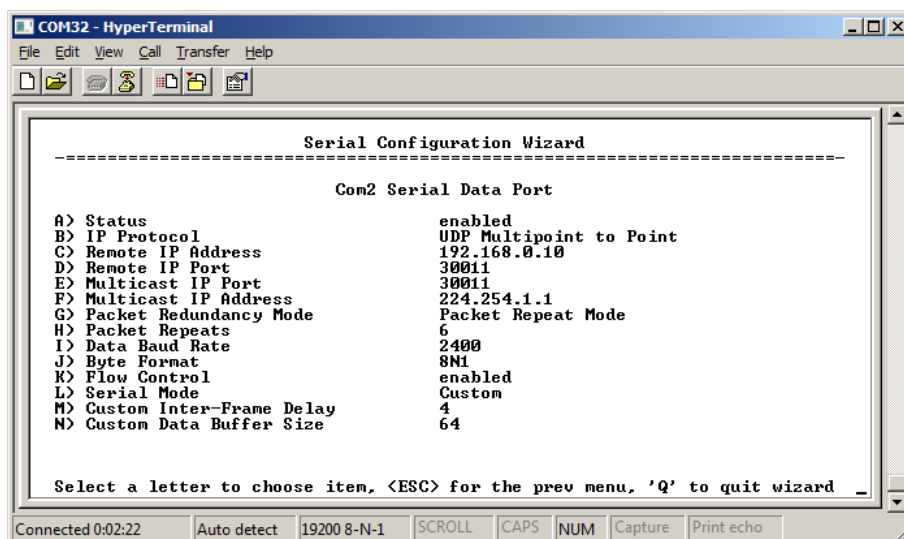


Figure 2-49. Remote Radio Serial Port Configuration

2.6.10 Point-to-Point Serial-to-Serial Application Example

Once the transceivers are configured and the changes have been executed, they begin processing any data presented at the COM ports. Data presented at the Access Point's COM port will be packetized and sent via UDP to the Remote. Upon receiving the packet, the Remote strips the data out of the UDP packet and sends it out its COM port. Likewise, data presented at the Remote's COM port is packetized, sent to the Access Point, stripped, and sent out the Access Point's COM port. This configuration does not use multicast addressing.

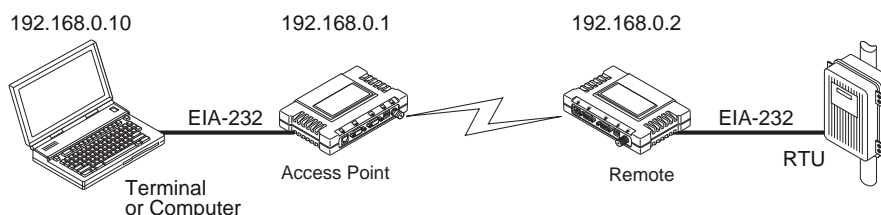


Figure 2-50. Point-to-Point Serial-to-Serial Application Diagram

Table 2-3. Serial Port Application Configuration

Transceiver Location	Menu Item	Setting
Access Point (COM2) ¹	Status	Enabled
	Data Baud Rate	9,600 (Example)
	Flow Control	Hardware (Example)
	Serial Mode	Seamless
	SIFD ²	4
	IP Protocol	UDP
	Remote IP Address	192.168.0.2 (IP address of the Remote radio)
	Remote IP Port	30011
	Local IP Port	30011

Table 2-3. Serial Port Application Configuration(Continued)

Transceiver Location	Menu Item	Setting
Remote Unit (COM2) ¹	Status	Enabled
	Data Baud Rate	9,600 (Example)
	Flow Control ³	ON/OFF (Example)
	Serial Mode	Seamless
	SIFD ²	4 (Characters)
	IP Protocol	UDP
	Remote IP Address	192.168.0.1 (IP address of the AP)
	Remote IP Port	30011
	Local IP Port	30011

1. Either COM port can be used, but they must be the same ones at both ends of the link. Both COM ports can be used simultaneously for two independent data channels.
2. Seamless Inter-frame Delay.
3. Flow Control applies to the COM2 Port only.

2.6.11 Combined Serial and IP Application Example

Note that in this example, the TCP mode does not involve the Access Point. Thus, the transceiver in a single network can run in *both* modes at the same time. In other words, some Remotes can be configured for TCP mode while others can be configured (along with the Access Point) for UDP mode.

In this configuration, the Host PC can use both data paths to reach the RTUs. This may be helpful when a mixed collection of RTUs is present where some RTUs can operate in a broadcast form while others cannot (see Figure 2-51 on Page 63 and Table 2-4 on Page 63).

Operation and Data Flow

- Communicate with RTU A by Telneting to Remote 1, port 30011.
- Communicate with RTU B by Telneting to Remote 2, port 30011.
- Communicate with RTUs C and D by sending and receiving data from the Access Point's COM port.
- All communication paths can be used simultaneously.

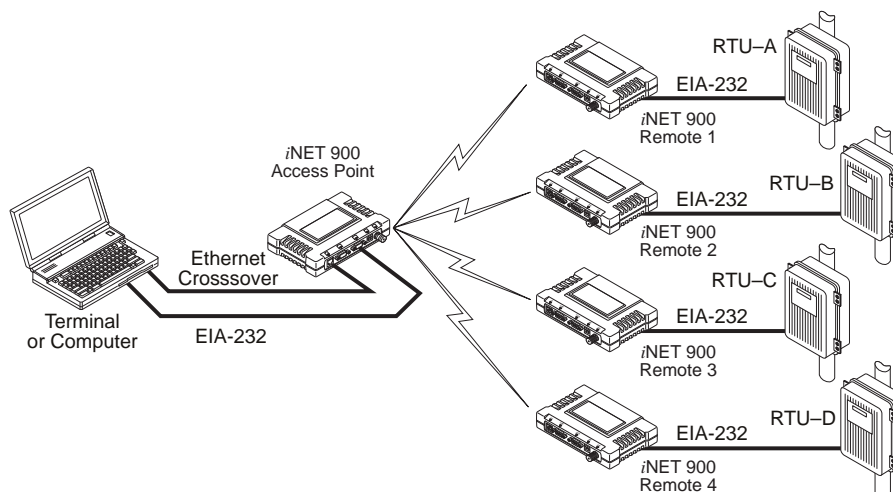


Figure 2-51. Mixed-Modes Application Diagram

Table 2-4. Serial Port Application Configuration

Transceiver Location	Menu Item	Setting
Access Point	Status	Enabled
	Baud Rate	9,600
	Flow Control	Disabled
	IP Protocol	UDP
	Send to Address	A multicast IP address such as 224.254.1.1
	Send to Port	30011
	Receive on Port	30011
	Receive on Address	0.0.0.0 (Not Used)
Remote Units 1 & 2 (COM2)	Status	Enabled
	Baud Rate	2,400
	Flow Control	Disabled
	IP Protocol	TCP
	Receive on Port	30011
Remote Units 3 & 4 (COM2)	Status	Enabled
	Baud Rate	9,600
	Flow Control	Disabled
	IP Protocol	UDP
	Send to Address	IP address of the AP
	Send to Port	30011
	Receive on Port	30011
	Receive on Address	224.254.1.1 (The multicast IP address used for the AP's Send To Address above)

2.6.12 Virtual LAN in iNET-II and iNET

The iNET-II and iNET radios support port-based VLAN at the Ethernet interface and over the air, as specified by the IEEE 802.1Q standard. VLAN settings are made on the **Network Interface Configuration Menu**. See “*Virtual LAN in iNET Series*” on Page 30 for more information.

2.7 Cyber Security Configuration

The cyber security features of the transceiver are grouped into three general areas: controlling access to the radio itself for configuration and management purpose (Device Security), controlling how and when radios communicate with each other, as well as how data traffic is handled (Wireless Security) and a special section dealing with authentication and authorization using a central server (RADIUS Configuration). Figure 2-52 shows the Security Configuration Menu, which is the entry point for these categories.

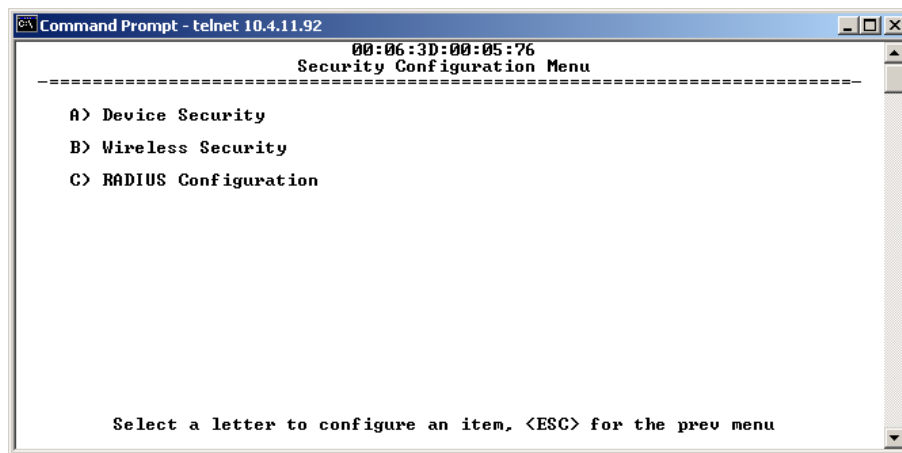


Figure 2-52. Security Configuration Menu
(Access Point Version Shown)

2.7.1 Device Security

This group of features controls how the radios can be accessed either locally or remotely for configuration and management.

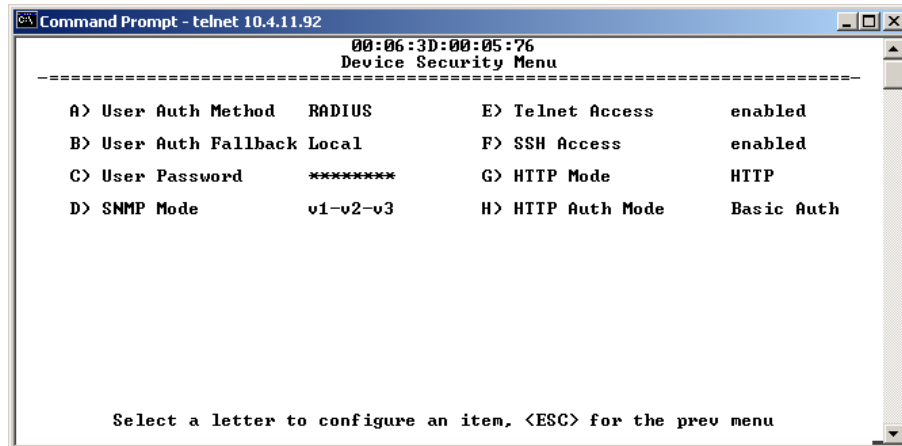


Figure 2-53. Device Security Menu

- **User Auth Method**— Defines whether username and password is verified locally or via a central server. [**Local**, **RADIUS**; **Local**]
- **User Auth Fallback**— Defines the alternate authentication mode in case the authentication server is not available. [**Local**, **None**; **Local**]
- **User Password**—Local password for this unit. Used at log-in via COM1 Port, Telnet, SSH and Web browser. [**Up to 8 alphanumeric characters without spaces (case-sensitive)**; **admin**]

TIP: For enhanced security, consider using misspelled words, a combination of letters and numbers, and a combination of upper and lower case letters. Also, the more characters used (up to eight), the more secure the password will be. These strategies help protect against sophisticated hackers who may use a database of common words (for example, dictionary attacks) to determine a password.

- **SNMP Mode**—This specifies the mode of operation of the radio's SNMP Agent. If the mode is disabled, the Agent does not respond to any SNMP traffic. If the mode is v1_Only, v2_Only, or v3_Only, the Agent responds only to that version of SNMP traffic. If the mode is v1-v2, or v1-v2-v3, the Agent responds to the specified versions of SNMP traffic. [**disabled**, **v1_Only**, **v2_Only**, **v3_Only**, **v1-v2**, **v1-v2-v3**; **v1-v2-v3**]
- **Telnet Access**—Controls remote access through Telnet sessions on Port 23 [**Enabled**, **Disabled**; **Enabled**]
- **SSH Access**— Controls remote access through SSH (Secure Shell) sessions on Port 22 [**Enabled**, **Disabled**; **Enabled**]
- **HTTP Mode**— Controls remote access through HTTP sessions on Ports 80 and 443. Selecting **HTTPS** forces secure connections to Port 443. When **HTTP Mode** is disabled, access through HTTP or HTTPS is not allowed. [**Disabled**, **HTTP**, **HTTPS**; **HTTP**]
- **HTTP Auth Mode**—Selects the method of HTTP log-in authentication. This parameter functions only when **HTTP** is selected in the previous menu item. Although the **Basic Auth** mode requests a password, the actual password text is transmitted in the clear (unencrypted). [**Basic Auth**, **MD5 Digest**; **Basic Auth**]

2.7.2 Wireless Security

The features in the Wireless Security menu control the communication of data across the wireless link. The radios can be authenticated locally via a list of authorized radios, or remotely via a centralized RADIUS server. RADIUS is a centralized authentication mechanism based on standards.

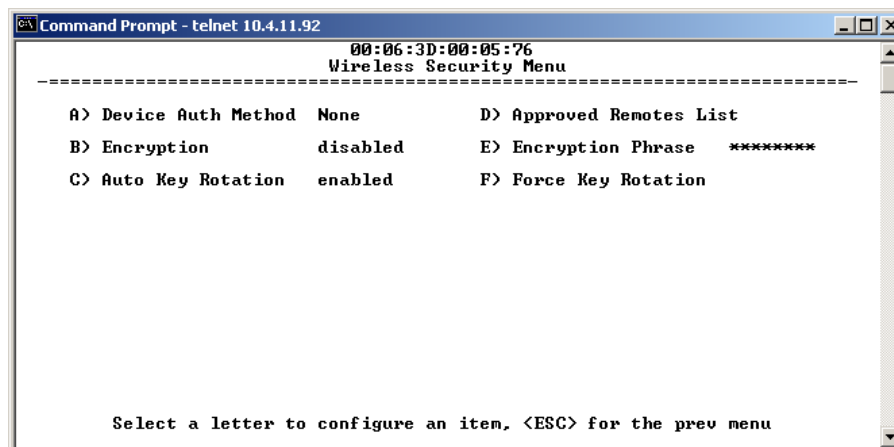


Figure 2-54. Wireless Security Menu, AP Menu

- **Device Auth Method**—Controls whether device authentication is executed locally, via a central server, or not at all. Selecting **Local** uses the Approved Remotes List described later in this manual. [**None**, **Local**, **IEEE 802.1X**; **None**]

- **Encryption**— When enabled, it forces the transceiver to use AES-128 encryption (RC4-128 on iNET) on all over-the-air messages. This option requires the Encryption Phrase to be previously configured. Both the AP and the Remote radios must use the same encryption phrase. (Some units may not be authorized to use encryption. “See “Authorization Key Menu” on Page 89” for additional details.) [Enabled, Disabled; Disabled]
- **Auto Key Rotation (AP only)**—When enabled, it forces the transceiver to use the key rotation algorithm to generate a new encryption key after 500 kilobytes of information has been transmitted, or one hour has elapsed. [Enabled, Disabled; Disabled]
- **Approved Access Points (RM only)/Remotes (AP only) List** —Displays a menu to manage the list of other radios with which this unit will be permitted to communicate.
- **Encryption Phrase**—Phrase (text & numbers) that will be used by the encryption algorithm. [8 to 29 alphanumeric characters; Blank]
- **Force Key Rotation (AP only)**— Triggers an immediate rotation of the encryption keys regardless of the internal rotation counters or the Auto Key Rotation setting being disabled.

Local Authentication—Approved Remotes/Access Points List Submenu

Setting the **Device Auth Method** to **Local** forces the transceiver to check the *Approved List* before a radio link can be established. In the case of a Remote, the AP must be in the *Approved Access Points List* before it accepts the beacon as being valid. In the case of an AP, a Remote must be in the *Approved Remotes List* to be granted authorization. **Device Auth Method Local** requires at least one entry in the list for successful association.

This menu is the same for both Access Points and Remotes and the names change to reflect their mode. Replace “Remotes” with Access Points” in the following description.

NOTE: The limit for Remotes (in an Access Point radio) is 255. The limit for Access Points (in a Remote radio) is 104.

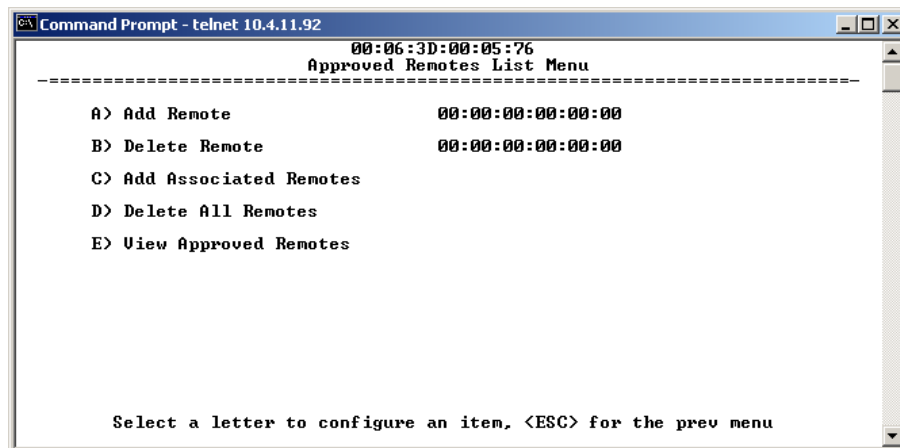


Figure 2-55. Approved Remotes List Menu (on AP)

- **Add Remote**—Enter MAC address of Remote. [Any valid 6-digit hexadecimal MAC address; 00:00:00:00:00:00]
- **Delete Remote**—Enter MAC address of Remote. For security purposes, you may want to delete a stolen or deprovisioned radio from this list.
- **Add Associated Remotes**—Add all currently associated remotes to the approved remote list. Alternatively, you can enter each Remote MAC manually.
- **Delete All Remotes**—Remove (complete purge) of all Remotes from current list.
- **View Approved Remotes**—Simple listing of approved Remotes by MAC address, of radios authorized to join this AP. If a Remote is not in this list, it will not be able to associate with this AP.
- **Save Changes**—Saves all changes made during the session with this menu. Changes are implemented only if they are “saved” before exiting this menu.

2.7.3 RADIUS Configuration

This section covers the authentication settings needed for the iNET radios to access the RADIUS server, which is used for Device Level Security and for Wireless Access Security. GE MDS does not provide the RADIUS server software.

Operation of Device Authentication

Device authentication forces the radio to authenticate before allowing user traffic to traverse the wireless network. When **Device Security** is configured to use IEEE 802.1X as the authentication method, Remote radios need three types of certificates: public (client), private, and root (Certificate Authority). These files are unique to each Remote radio and need to first be created at the server and then installed into each unit via TFTP. The certificate files must be in DER format.

Device authentication uses the serial number of each radio as the Common Name (CN) in its certificate and in its RADIUS identity field. Each Access Point *and* Remote radio must be identified/recognized by the RADIUS Server through the Common Name (Serial number) and IP address entries.

NOTE: Consult your RADIUS network administrator for assistance in configuration, or for help with other issues that may arise.

To activate device authentication, select **Device Auth Method** and set **IEEE 802.1X** as the active mode. The behavior of this setting differs depending on whether it is implemented on an Access Point or a Remote transceiver. An explanation of these behaviors is given below:

Access Point: When **Device Auth Method** is set to **IEEE 802.1X**, the AP disassociates all associated Remotes and waits for the RADIUS Server to Authenticate the Remotes before allowing data to be passed from them. When approval is received from the RADIUS Server, data from the Remote is allowed to pass.

Remote: When **Device Auth Method** is set to **IEEE 802.1X**, the Remote halts any data it is passing, and requests Authentication from the RADIUS Server. If accepted, data is allowed to be transmitted. The Access Point that the Remote connects to must have a valid RADIUS configuration and connection to the configured RADIUS server.

Operation of User Authentication

When user authentication is set to **Local** or **RADIUS**, you must enter a valid user name and password before being allowed to manage the radio. In **RADIUS** mode both of these fields may be up to 40 characters long. In **Local** mode the user name is **iNET** and the password may be up to 8 characters long.

When set to **RADIUS**, *all* logins to the local configuration services are required to be authenticated via the RADIUS Server, including telnet and SSH (Secure Shell) sessions. Authentication must be accepted before access to the radio menu is granted.

2.7.4 RADIUS Configuration

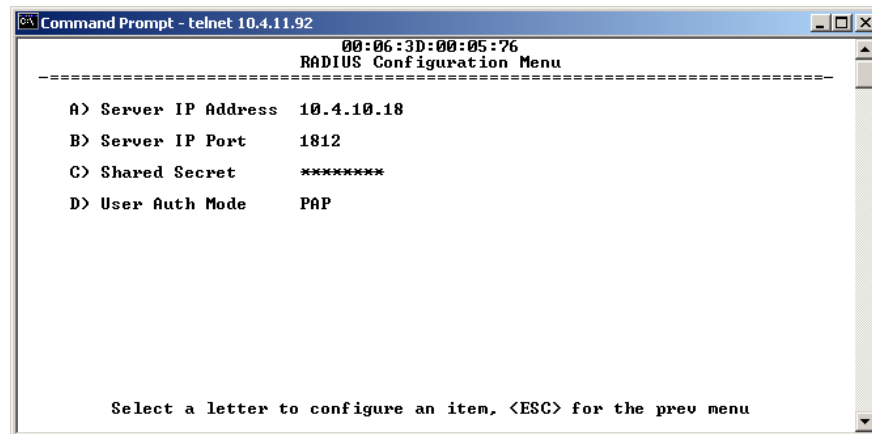


Figure 2-56. RADIUS Configuration Menu

- **Server IP Address**—Used to set/display address of the Server where the RADIUS application resides.
- **Server IP port**—1812 is the standard port for authentication (RFC 2865, June 2000), but this setting may be changed if necessary to any number between 1 and 65535. [**1-65535; 1812**]
- **Shared Secret**—User authentication and Device authentication require a common shared secret to complete a RADIUS transaction. This entry must match the string used to configure the appropriate files on the RADIUS Server. [**8 to 29 alphanumeric characters**]
- **User Auth Mode**—Should be set to PAP or CHAP depending on the configuration of the server. [**PAP, CHAP; PAP**]

NOTE: CHAP is more secure than PAP. PAP may display the login password in log files at the RADIUS Server while CHAP will encrypt the login password.

NOTE: The security password may not exceed 40 characters in length.

2.7.5 Certificate Management *(Remote transceivers only)*

Use Certificate generation software to generate certificate files and then install these files into each Remote unit via TFTP. The certificate files must be in DER format. The Common Name (CN) field in the public certificate file must match the serial number of the unit it will be installed in.

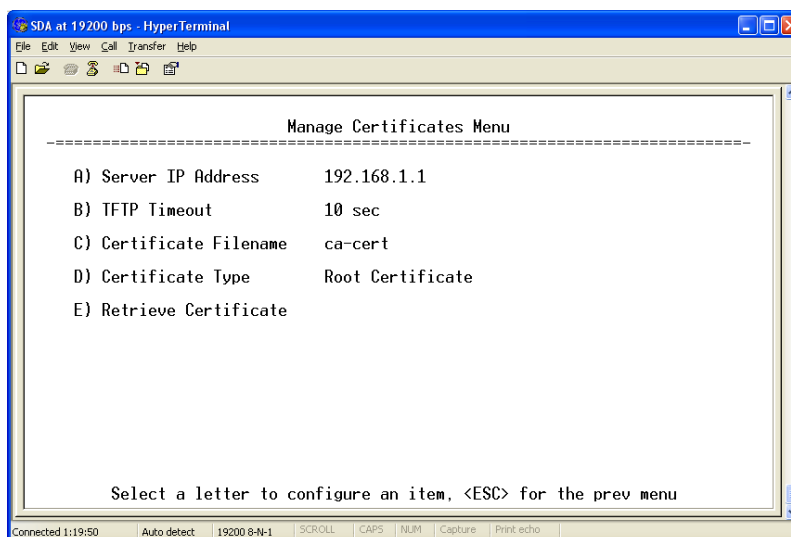


Figure 2-57. Manage Certificates Menu

- **Server IP Address**—the IP address of the Server where the RADIUS application resides.
- **TFTP Timeout** should be set appropriately according to the layout of the network.

Three certificate files (Root, Client, and Private Key) must be present in *each* of the Remote radios. Use the commands described below to install these files into each Remote radio.

- **Certificate Filename**—Used to specify the filename of the certificate file residing on the TFTP server.
- **Certificate Type**—Selects one of the three file types mentioned above. [**Root Certificate, Client Certificate, Private Key Certificate; Root Certificate**]
- **Retrieve Certificate**—Initiates the retrieval of the certificate file from the storage location. A successful installation issues a **Complete** status message.

NOTE: It is *imperative* that the three certificate files are installed correctly into the Remote radio, in their respective file types. If they are not, it will render the Remote un-authenticated for data traffic. Consult your RADIUS network administrator if issues arise.

The radio will individually check that each certificate loaded matches the file type chosen (for example, Private Key Certificate, Client Certificate, or Root Certificate). Once all certificates are loaded, the radio performs a certificate chain verification.

If new certificates must be installed to a radio with previously installed certificates, load the root CA certificate first. This will remove the private key and client certificates from the radio. Otherwise, attempting to load a new certificate that has a different root certificate will be denied by the radio because of failing the certificate chain validation.

2.8 Performance Verification

After the basic operation of the radio has been checked, you may wish to optimize the network's performance using some of the following suggestions. The effectiveness of these techniques will vary with the design of your system and the format of the data being sent.

There are two major areas for possible improvement—the radio and the data network. The following sections will provide you with a variety of items to check and on many occasions, ways to correct or improve their performance.

The menu/screen shown in Figure 2-58 is one of two primary sources of information on the radio layer and radio network performance.

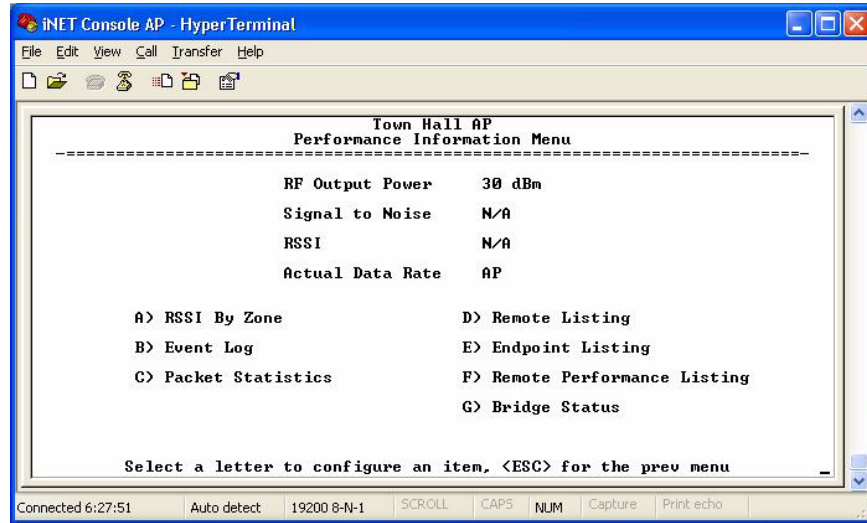


Figure 2-58. Performance Information Menu
(AP Version Shown)

- **RF Output Power** (*Display only*)—Measured power output. (See “How Much Output Power Can be Used?” on Page 112)
- **Signal-to-Noise** (*Display only*)—Current running-average SNR value all active operating frequencies. (No value displayed on APs)

NOTE: The RSSI is an average of the last 20 RSSI samples. The RSSI value is reset every time the radio returns to scanning mode.

- **RSSI** (*Display only*)—Current running-average Received Signal Strength Indication for all active operating frequencies. (No value displayed on APs.)
- **Actual Data Rate** (*Display only*)—Over-the-air transmission rate (as opposed to selected data rate) for the remote being monitored. The fastest data rates can generally be achieved with stronger signal levels.
- **RSSI by Zone**—Received Signal Strength Indicator by Zone. (See “RSSI by Zone Menu (Remotes Only)” on Page 71)
- **Event Log**—Access the menu for managing the unit’s log of operational activities. See “Authorization Key Menu” on Page 89.
- **Packet Statistics**—Multiple radio and network operating statistics. (See “Packet Statistics Menu” on Page 74)
- **Wireless Network Status** (*Displayed only at Remotes*)—Current association state and MAC address of the Access Point. (See “Wireless Network Status (Remotes Only)” on Page 76)
- **Remote Listing** (*AP Display only*)—List of basic information for all Remote units currently associated with this Access Point. (See “Remote Listing Menu (Access Points Only)” on Page 78)
- **Endpoint Listing** (*AP Display only*)—List of units accessible by this AP through associated Remote ports. (See “Endpoint Listing Menu (Access Points Only)” on Page 79)
- **Remote Performance Listing** (*AP Display only*)—(See “Remote Performance Listing Menu (Access Points Only)” on Page 80)
- **Bridge Status**—Displays the network bridge status. See “Bridge Status Menu” on Page 81.

2.8.1 RSSI by Zone Menu *(Remotes Only)*

This screen displays the strength of RF signals received from the currently associated Access Point.

Network integrity depends in large part on stable radio signal levels being received at each end of a data link. In general, signal levels stronger than –80 dBm will provide reliable communication that includes a 15 dB fade margin.

If you find there is a poor signal level on one zone, check the section 2.8.3 on page 74 and record the values. Then, set the questionable zone to “Skipped” in the Radio Configuration Menu (page 40) and look for an improvement in the Packet Statistics error rates. If there is none, return the Zone to “Active.”

RSSI measurements and Wireless Packet Statistics are based on multiple samples over a period of several seconds. The average of these measurements will be displayed by the Management System.

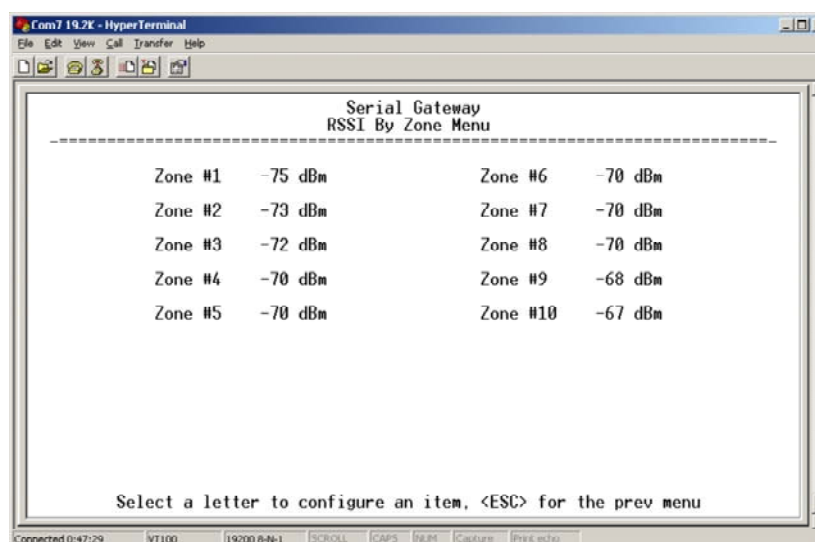


Figure 2-59. RSSI by Zone Menu

TIP: Under normal circumstances, the signal levels in each zone should be within a few decibels of each other. If you see one that is significantly lower or higher, it may be a sign of radio frequency interference from another signal source on the 900 MHz band. See “Performance Notes” on Page 117 for information that can help you minimize radio frequency interference.

2.8.2 Event Log Menu

The transceiver’s microprocessor monitors many operational parameters and logs them. Events are classified into four levels of importance, which are described in Table 2-5. Some of these events result from a condition preventing normal operation of the unit—these are “critical” events. These will cause the unit to enter an “alarmed” state and the PWR LED to blink until the condition is corrected. All events are stored in the Event Log that can hold up to 9,000 entries.

Table 2-5. Event Classifications

Level	Description/Impact
Informational	Normal operating activities
Minor	Does not affect unit operation
Major	Degraded unit performance but still capable of operation
Critical	Prevents the unit from operating

Time and Date

The events stored in the Event Log are time-stamped using the time and date of the locally connected device. Remote units obtain this information from the Access Point when they associate with it. The Access Point obtains the time and date from a Time Server. This server can generally be provided by a standard Windows PC server SNTP application. In the absence of the SNTP services, the user must manually enter it at the Access Point. (See “Device Information” on Page 25 for SNTP server identification.) The manually set time and date clock is dependent on the unit’s primary power. A loss of power will reset the clock to January 1, 2002 but will not affect previously stored error events.

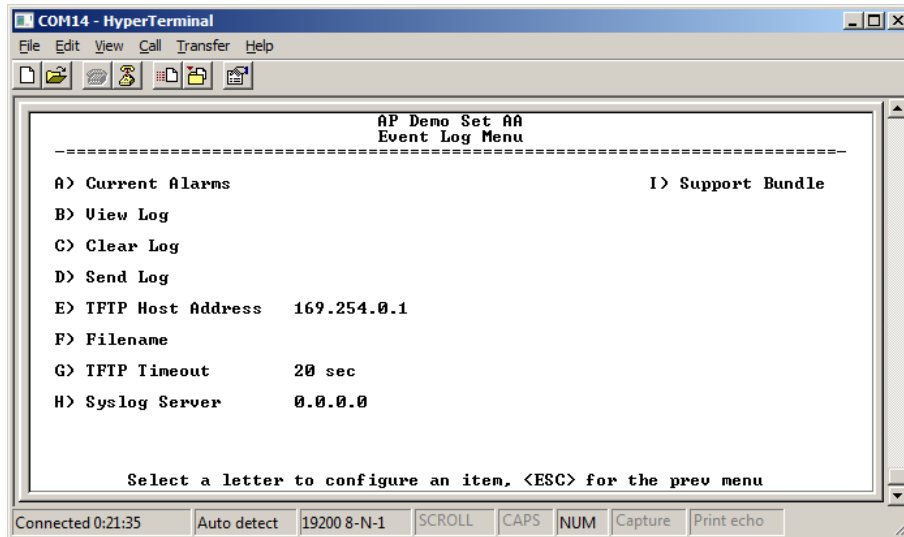


Figure 2-60. Event Log Menu

- **Current Alarms**—View list of root causes that have placed the Device Status in the alarmed state. (See “Alarm/Event Conditions” on Page 99)
- **View Log**—View a list of events stored in the current log. Some of these events are stored in volatile memory and will be erased with a loss of power. The events are numbered for easier identification and navigation.
- **Clear Log**—Purges the log of all events.

TIP: Save your Event Log before choosing to clear it in order to retain potentially valuable troubleshooting information. (See “Upgrading the Firmware” on Page 84 for an overview on how to transfer files from the transceiver to a computer on the network using TFTP.)

- **Send Log**—Initiate TFTP transfer of the unit’s event Event Log in a plain text (ASCII) file to a TFTP server at the remote location.
- **TFTP Host Address**—IP address of the computer on which the TFTP server resides. This same IP address is used in other screens/functions (reprogramming, logging, etc.). Changing it here also changes it for other screens/functions. [**Any valid IP address; 127.0.0.1**]
- **Filename**—Name to be given to the Event Log file sent to the TFTP server for archiving. [**Any 40-char alphanumeric string; Blank**]

NOTE: You might want to change the filename to reflect the type of log you intend to archive and/or its date.

- **TFTP Time-out**—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the transceiver before canceling the file transfer. [**10 to 120 seconds; 10**]
- **Syslog Server**—IP address to which alarms are sent using the syslog message format. [**Any valid IP address; 0.0.0.0**]

- **Support Bundle**—GEMDS debug file containing system information helpful in radio debugging. See “Support Bundle” on Page 92.

View Current Alarms

Most events, classified as “critical” will make the PWR LED blink, and will inhibit normal operation of the transceiver. The LED will remain blinking until the corrective action has been completed.

An alarm condition is different from a log event in the sense that an alarm is persistent in nature. That is, an alarm condition remains as an alarm until it has been cleared by correcting the cause (see Table 3-6 on Page 100 for corrective action).

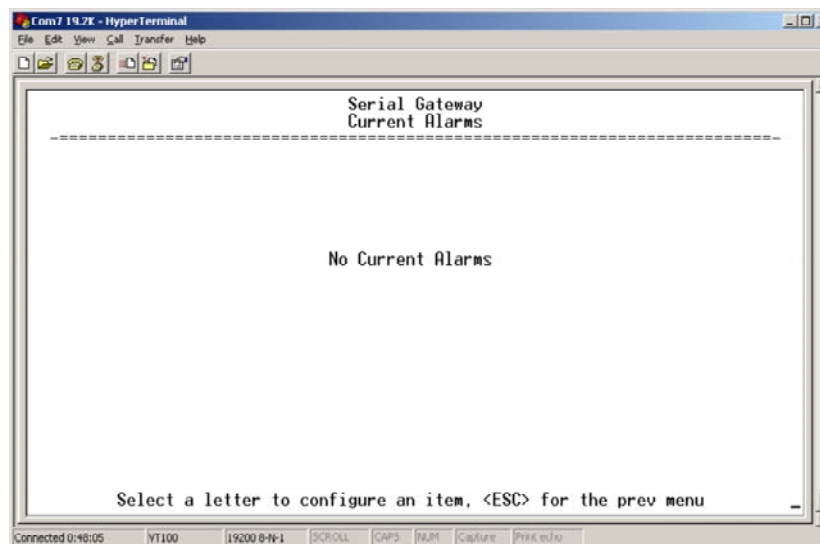


Figure 2-61. Current Alarms Screen

View Event Log

Event classifications are listed starting in Table 3-4 on Page 99 to Table 3-7 on Page 102.

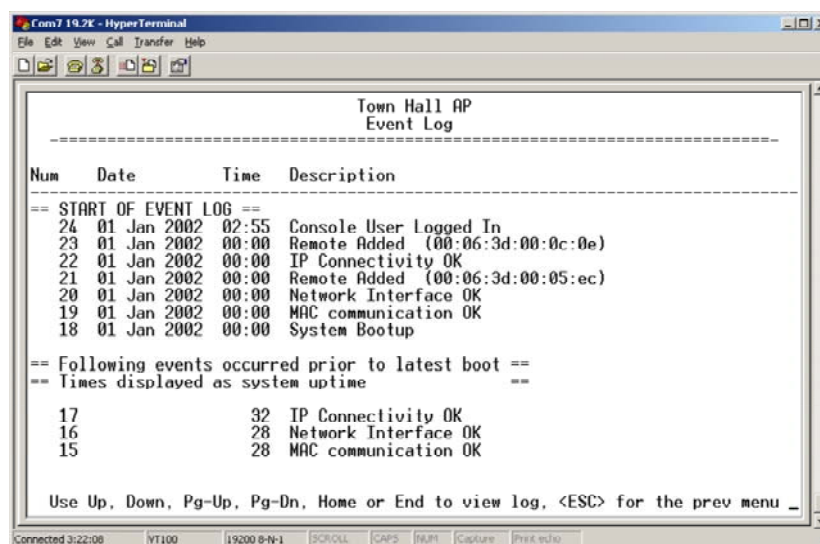


Figure 2-62. Sample Event Log Screen

2.8.3 Packet Statistics Menu

An iNET radio maintains running counters of different categories of events in the Ethernet protocol. The Packet Statistics refer to each Ethernet interface from the perspective of the *radio*.

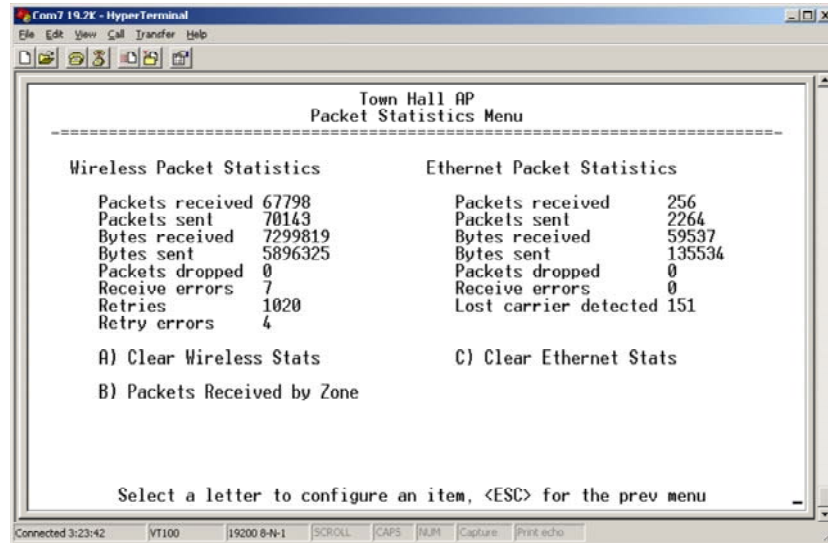


Figure 2-63. Sample Packet Statistics Menu

Wireless Packet Statistics

- **Packets received**—Over-the-air data packets received by this unit.
- **Packets sent**—Over-the-air data packets sent by this unit.
- **Bytes received**—Over-the-air data bytes received by this unit.
- **Bytes sent**—Over-the-air data bytes sent by this unit.
- **Packets dropped**—To-be-transmitted packets dropped as a result of a lack of buffers in the RF out-bound queue.
- **Receive errors**—Packets that do not pass CRC. This may be due to transmissions corrupted by RF interference.
- **Retries**—Number of requests to re-send a data packet before it is acknowledged. If the packet was not acknowledged, this counter is not incremented.
- **Retry errors**—Packets discarded after exceeding seven retries over-the-air.
- **Clear Wireless stats**—Resets the statistics counter.

Ethernet Packet Statistics

- **Packets received**—Packets received by the transceiver through the Ethernet port.
- **Packets sent**—Packets transmitted by the transceiver through the Ethernet port.
- **Bytes received**—Data bytes received by this unit through its LAN port.
- **Bytes sent**—Data bytes sent by this unit through its LAN port.
- **Packets dropped**—Received packets dropped as a result of a lack of buffers.
- **Receive errors**—Packets that do not pass CRC. This may be due to collisions in the Ethernet LAN.
- **Lost carrier detected**—A count of the number of packets that the unit attempted to send out the Ethernet port when the carrier signal of the Ethernet was not present. (No carrier present could be due to a loose connection, bad or wrong cable, or equipment failure at the other end of the Ethernet cable.)
- **Clear Ethernet stats**—Resets the statistics counter.
- **Wireless Packet Statistics** (when VLAN is shown)—A screen almost identical to Figure 2-63 is shown, except that option D (VLAN Packet Stats) appears as in Figure 2-64 on Page 75.

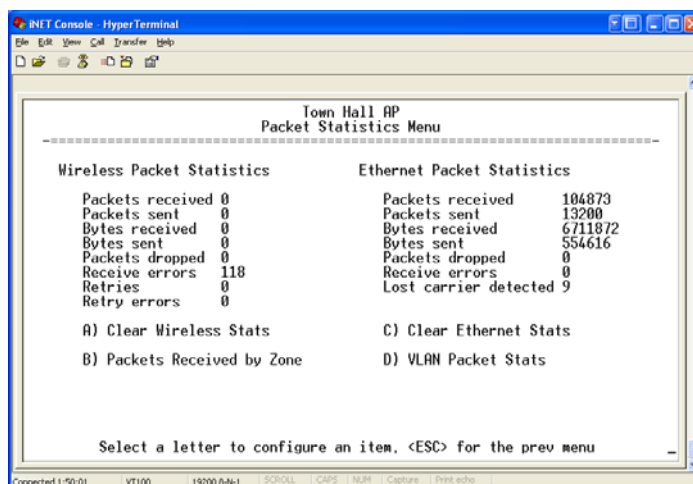


Figure 2-64. Sample Packet Statistics Menu

The VLAN Packet Statistics Menu (Figure 2-65) groups the statistics of both wired and wireless interfaces. The numbers have different meaning depending on whether the Ethernet port is defined as an Access Port or as a Trunk Port.

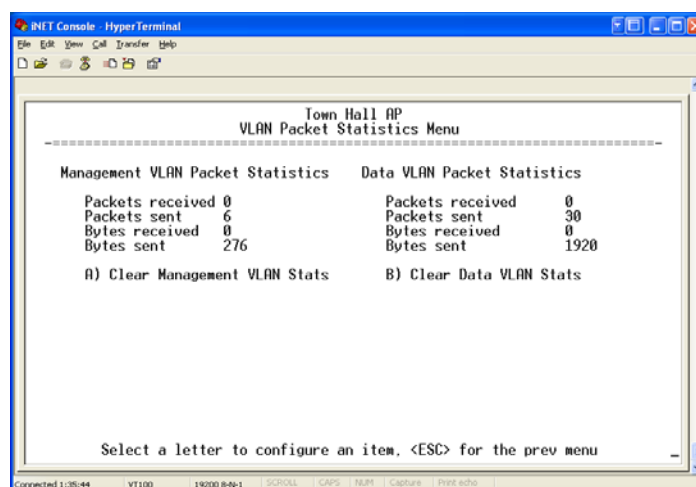


Figure 2-65. VLAN Packet Statistics

Packets Received by Zone

This screen, shown in Figure 2-66, presents a breakdown of wireless packet statistics by-zone. All zones should report similar numbers. If one or more zones report lower numbers than the others (2% reduction), the specific zone is probably experiencing interference. An improvement can be realized by blocking this zone (see **Main Menu>>Radio Configuration>>Skip Zone Option**).

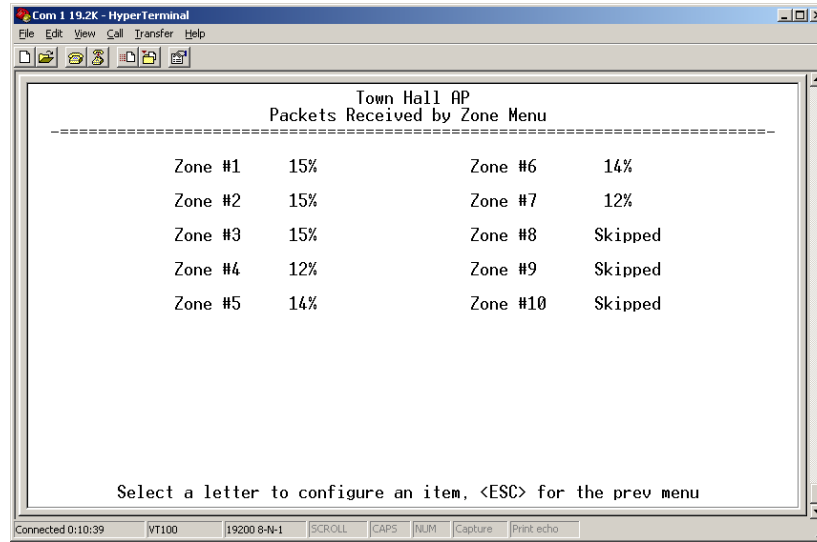


Figure 2-66. Packets Received By Zone Menu

2.8.4 Wireless Network Status *(Remotes Only)*

The Wireless Network Status screen provides information on a key operating process of the transceiver—the association of the Remote with the Access Point. The following is a description of how this process takes place and as monitored on Figure 2-67, “. Wireless Network Status Screen (Remotes Only),” on page 77.

The Transceiver’s Association Process

After the Remote is powered up and finishes its boot cycle, it begins scanning the 900 MHz band for beacon signals being sent out from AP units. If the Remote sees a beacon with a *Network Name* that is the same as its own, the Remote will stop its scanning and temporarily synchronize its frequency-hopping pattern to match the one encoded on the AP’s beacon signal. The Remote waits for three identical beacon signals from the AP and then it toggles into a fully synchronized “associated” state. If the Remote does not receive three identical beacons from the Access Point unit within a predetermined time period, it returns to a scanning mode and continues to search for an AP with a matching network name in its beacon.

Under normal circumstances, the association process should be completed within 20 seconds after boot-up. This time can vary depending on the beacon period setting on the AP, and the beacon learning setting on the Remote. Refer to **Beacon Period** and **Beacon Learning** descriptions in “Radio Configuration Menu” on Page 40.

Remote units are always monitoring the beacon signal. If an associated Remote loses the AP’s beacon for more than 20 seconds, the association process starts again.

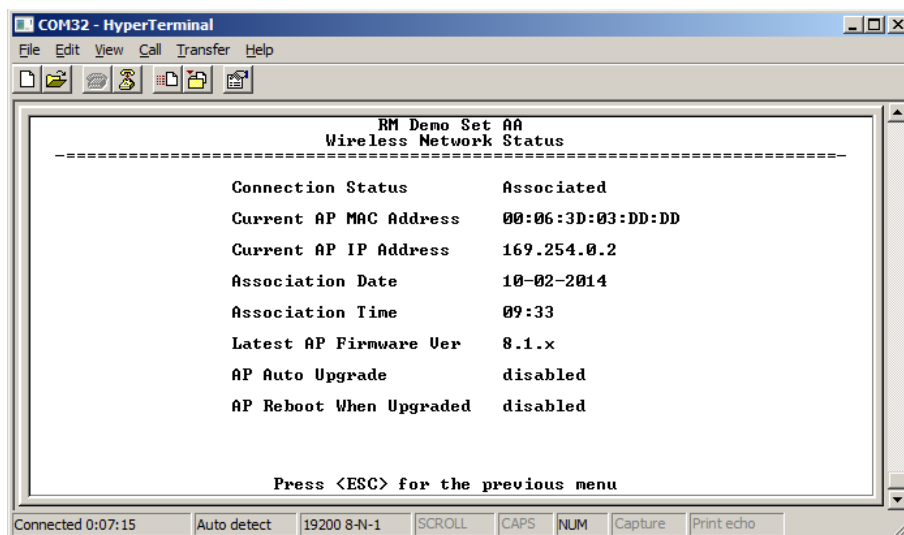


Figure 2-67. Wireless Network Status Screen (Remotes Only)

- **Connection Status**—Current state of the wireless network communication.
 - *Scanning*—The unit is looking for an Access Point beacon signal.
 - *Exp(ecting) Sync(hronization)*—The unit has found a valid beacon signal for its network.
 - *Hop Sync*—The unit has changed its frequency hopping pattern to match that of the Access Point.
 - *Connected*—The unit has established a radio (RF) connection with the Access Point, but has not obtained cyber-security clearance to pass data. See “Operation of Device Authentication” on Page 67.
 - *Associated*—This unit has successfully synchronized and associated with an Access Point. This is the normal status.
 - *Alarmed*—The unit has detected one or more alarms that have not been cleared.
- **Current AP MAC Address**—Wireless address of Access Point with which the Remote is associated.
- **Current AP IP Address**—IP address of Access Point with which the Remote is associated.
- **Association Date**—Date of last successful association with an Access Point.
- **Association Time**—Time of day association was established on the association date.
- **Latest AP Firmware Version**—Displays the first two digits of the associated AP’s firmware.
- **AP Auto Upgrade**—Displays if the associated AP’s over-the-air reprogramming parameter is enabled or disabled.
- **AP Reboot when Upgraded**—Displays if the associated AP’s parameter for rebooting the Remotes after over-the-air reprogramming is enabled or disabled.

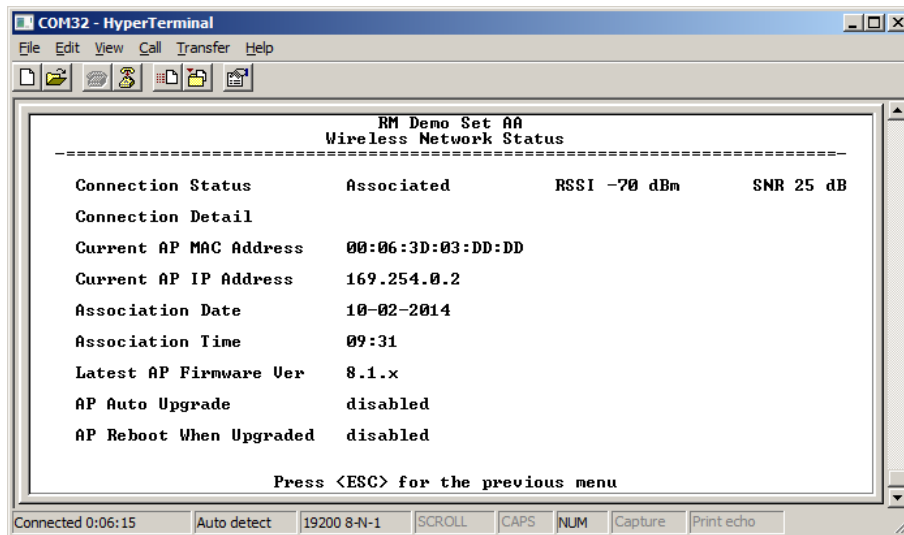


Figure 2-68. Wireless Network Status Screen with Mobility Enabled (Remotes Only)

When mobility is enabled, these additional read-only parameters will be available:

- **Connection Detail**—This value is only populated when the Connection Status is in **Scanning** and for a limited time after **Association**.
 - **RSSI assoc threshold** is when scanning begins after falling below the disassociation threshold.
 - **RSSI assoc threshold now** is when an association threshold back-off step is applied.
 - **RSSI assoc threshold reset to** is when the blacklist timer expires and the AP that has been black-listed is added back into the scan list.
- **RSSI**—Current average RSSI value in dBm.
- **SNR**—Current average Signal to Noise Ratio (SNR) value in dB.

2.8.5 Remote Listing Menu (Access Points Only)

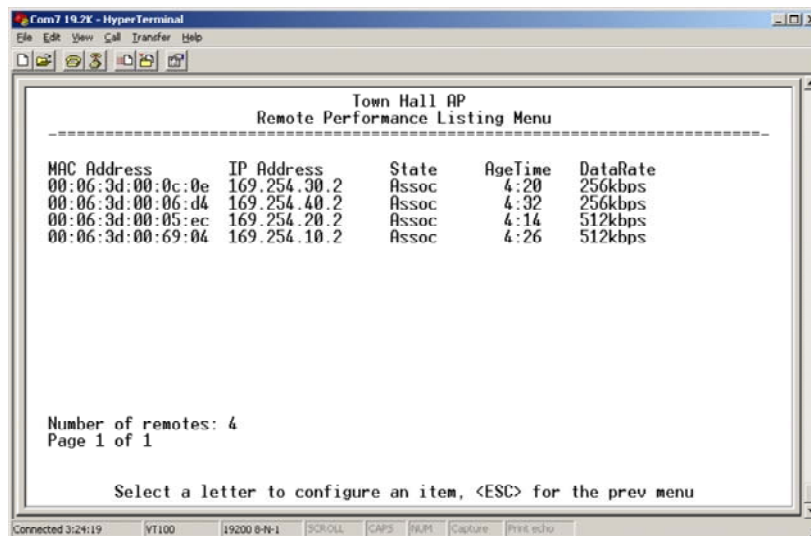


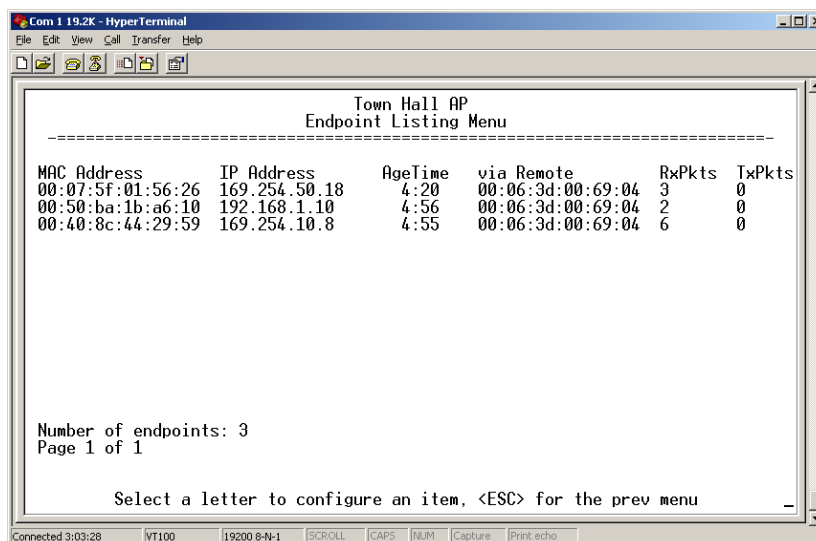
Figure 2-69. Remote Listing Menu
(List of transceivers associated with this AP)

- **MAC Address**—Hardware address of the Remote transceiver.
- **IP Address**—IP Address of the Remote transceiver.

- **State**—Current association state of the Remote transceiver.
- **AgeTime**—Time, in minutes, remaining before the device (address) will be deleted from the table. Each AP maintains a table with the addresses of the remote radios it communicates with. The age-time countdown is restarted to the configured Database Timeout setting (located in the Network Configuration; see “*Network Configuration Menu*” on Page 27) every time a message to/from that remote is detected. If no traffic is exchanged with that remote, it then “ages out” of the table. When traffic is detected it is included again in the table. This optimizes memory space utilization.
- **DataRate**—The current supported data rate of this unit.

2.8.6 Endpoint Listing Menu (*Access Points Only*)

This list shows all of the non-iNET 900 Ethernet devices that are known to the transceiver and is equivalent to the ARP table of IP devices.



MAC Address	IP Address	AgeTime	via Remote	RxPkts	TxPkts
00:07:5f:01:56:26	169.254.50.18	4:20	00:06:3d:00:69:04	3	0
00:50:ba:1b:a6:10	192.168.1.10	4:56	00:06:3d:00:69:04	2	0
00:40:8c:44:29:59	169.254.10.8	4:55	00:06:3d:00:69:04	6	0

Number of endpoints: 3
Page 1 of 1

Select a letter to configure an item, <ESC> for the prev menu

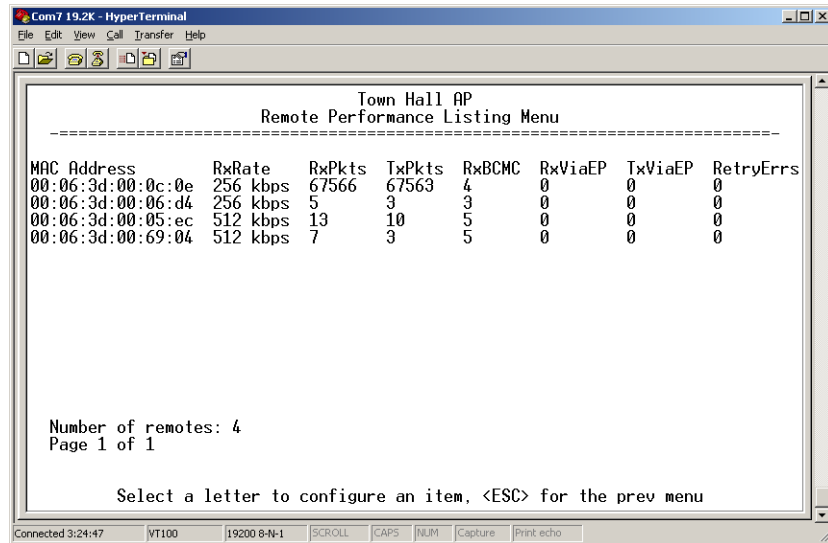
Figure 2-70. Endpoint Listing Menu
(Lists all equipment attached to REMOTE transceivers in the network)

- **MAC Address**—MAC address of each Endpoint connected via each Remote.
- **IP Address**—IP Address of endpoint device.
- **AgeTime**—Time, in minutes, remaining before the device (address) will be deleted from the table.

Each transceiver maintains a table with the addresses of the device it communicates with. The age-time countdown is restarted to the configured Database Timeout setting (located in the Network Configuration; see “*Network Configuration Menu*” on Page 27) every time a message to/from that remote is detected. If no traffic is exchanged with that remote, it then “ages out” of the table. When traffic is detected it is included again in the table. This optimizes memory space utilization.

- **via Remote**—Hardware address of the radio connected to this device.
- **RxPkts**—Over-the-air data packets received by the transceiver, and passed on to the endpoint device.
- **TxPkt**—Number of packets received from the endpoint device and passed over-the-air.

2.8.7 Remote Performance Listing Menu *(Access Points Only)*



MAC Address	RxRate	RxPkts	TxPkts	RxBCMC	RxViaEP	TxViaEP	RetryErrs
00:06:3d:00:0c:0e	256 kbps	67566	67563	4	0	0	0
00:06:3d:00:06:d4	256 kbps	5	3	3	0	0	0
00:06:3d:00:05:ec	512 kbps	13	10	5	0	0	0
00:06:3d:00:69:04	512 kbps	7	3	5	0	0	0

Number of remotes: 4
Page 1 of 1

Select a letter to configure an item, <ESC> for the prev menu

Figure 2-71. Remote Performance Listing Menu for iNET AP
(iNET-II will show RxRate as 512 kbps or 1024 kbps)

This screen provides a unit-by-unit summary of all Remote units currently associated with this Access Point. The parameters are displayed in a column format with each line corresponding to one Remote.

- **MAC Address**—Wireless MAC Address of each Remote to which the AP communicates.
- **RxRate**—Over-the-air data rate the radio is currently using. Transceivers may use different rates.
- **RxPkts**—Over-the-air data packets received from this unit.
- **TxPkts**—Over-the-air data packets sent to this unit.
- **RxBCMC**—Total number of Broadcast and/or Multicast packets received over-the-air.
- **RxViaEP**—Packets received by the transceiver through the Ethernet port.
- **TxViaEP**—Packets sent by the transceiver through the Ethernet port.
- **RetryErrs**—Packets discarded after exceeding five retries over-the-air.

2.8.8 Bridge Status Menu

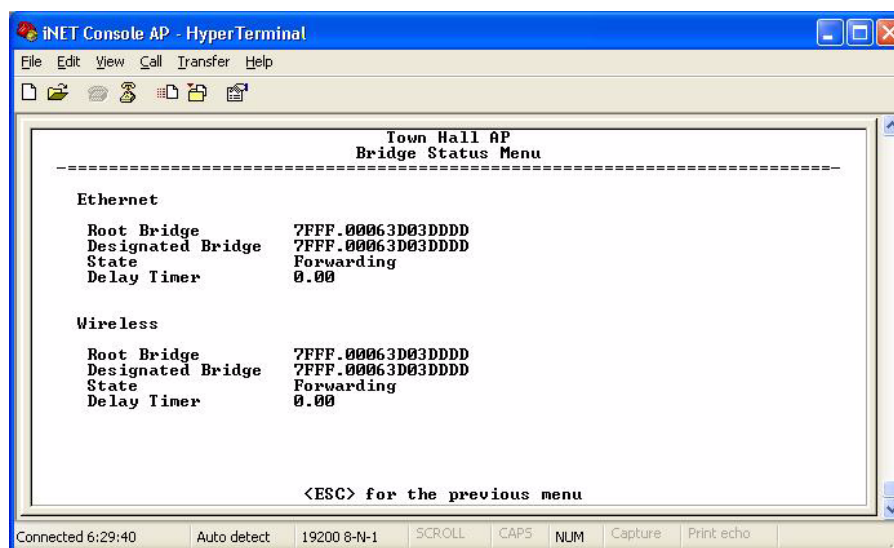


Figure 2-72. Bridge Status Menu
(all values are read only)

2.8.9 Serial Data Statistics Menu

This screen provides a summary of port activity for both serial data ports. These values will be reset to zero after a reboot cycle.

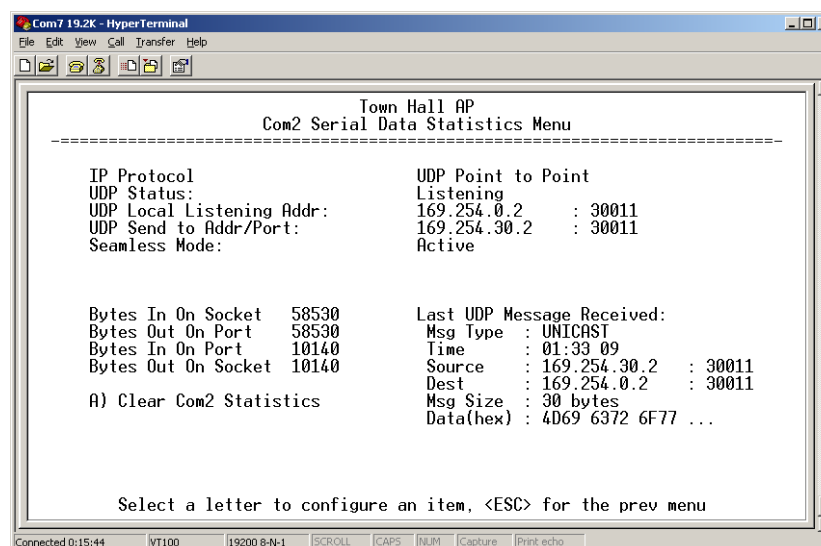


Figure 2-73. Serial Data Statistics Screen
(COM2 statistics shown; COM1 statistics will look similar)

- **Bytes in on socket**—Number of bytes received by the transceiver through the IP socket
- **Bytes out on port**—Number of bytes transmitted by the transceiver through the serial interface
- **Bytes in on port**—Number of bytes received by the transceiver through the serial interface

- **Bytes out on socket**—Number of bytes transmitted by the transceiver through the IP socket

In general, the number of bytes **Out on Socket** should follow the number of bytes **In On Port** as all bytes received on the serial port should be transmitted out to the IP interface. The same should be true in the opposite direction, bytes **Out On Port** should follow bytes **In On Socket**.

- **Clear Com1/2 Statistics**—Resets counter to zero.

2.9 Maintenance

In the normal course of operating a wireless network, you will want to take advantage of product improvements, and to read and archive the configuration of your individual transceivers using the *Maintenance / Tools Menu*. This section provides detailed information on how to take advantage of these services.

The maintenance tasks are:

- **Reprogramming**—Managing and selecting the unit's operating system firmware resources. (See "Reprogramming Menu" on Page 83)
- **Configuration Scripts**—Saving and importing data files containing unit operating parameters/settings. (See "Configuration Scripts Menu" on Page 87)
- **Authorization Key**—Alter the unit's overall capabilities by enabling the built-in resources. (See "Authorization Key Menu" on Page 89)

NOTE: Authorization keys are provided by a GE MDS technical representative. Call GE MDS if you want to alter your unit's capabilities.

- **Auto-Upgrade/Remote-Reboot (AP only)**—Configure when remotes retrieve new firmware versions from the associated AP, and whether or not they reboot to the new firmware after receiving the new firmware. (See "Auto-Upgrade/Remote-Reboot Menu" on Page 90)
- **Radio Test**—A diagnostic tool for testing RF operation. (See "Radio Test Menu" on Page 90)
- **Ping Utility**—Diagnostic tool to test network connectivity. (See "Ping Utility Menu" on Page 92)
- **Reset to Factory Defaults**—See "Reset to Factory Defaults" on Page 92.
- **Support Bundle**—Logs for radio debugging. (See "Support Bundle" on Page 92).

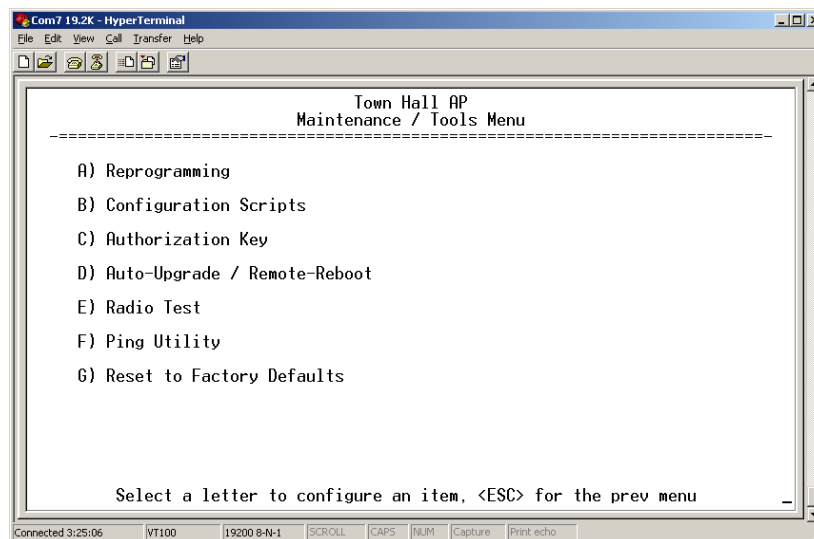


Figure 2-74. Maintenance/Tools Menu
(AP image shown)

2.9.1 Reprogramming Menu

The transceiver has two copies of the firmware (microprocessor code) used for the operating system and applications. One copy is “active” and the second one is standing by, ready to be used once activated. You can load new firmware into the inactive position and place it in service whenever you desire.

From time-to-time GE MDS offers upgrades to the transceiver firmware. Loading new firmware into the unit will not alter any privileges provided by Authorization Keys and does *not* require the transceiver be taken off-line until you want to operate the unit from the newly installed firmware image.

Firmware images are available free-of-charge at www.gemds.com.

NOTE: MDS iNET firmware may *not* be installed in MDS iNET-II radios, or vice-versa.

NOTE: When upgrading to firmware 6.0.0 or later, the unit creates internal files following the first reboot. This one-time process delays the response of the HTTP interface for 5-10 minutes. If DC power is cycled (turned off and back on) during this process, the files will have to be created again. It is recommended that you wait until this 5-10 minute process is complete before verifying operation of HTTP, HTTPS, or SSH.

NOTE: Always read the release notes for downloaded firmware. Some versions may not be compatible over the air, or with the particular unit you have.

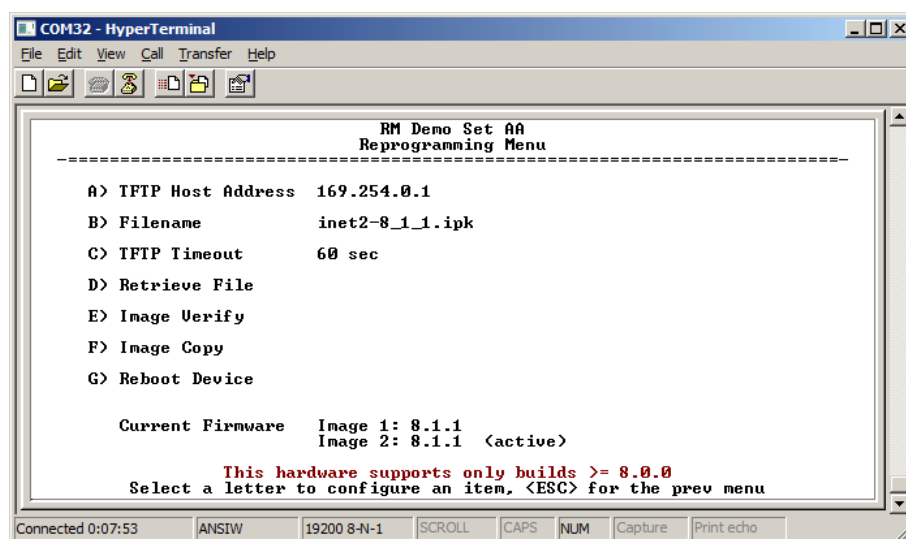


Figure 2-75. Reprogramming Menu

- **TFTP Host Address**—IP address of the host computer from which to get the file. [Any valid IP address] This same IP address is used in other screens/functions (reprogramming, logging, and so on). Changing it here also changes it for other screens/functions.
- **Filename**—Name of file to be received from the TFTP server. [Any 40-character alphanumeric string] Verify that this corresponds to the TFTP directory location. May require sub-directory, for example: **Firmware\inet\inet-4_4_0.ipk**.
- **TFTP Timeout**—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the *transceiver* before canceling the file transfer. [2 to 60 seconds; 10]
- **Retrieve File**—Initiates the file transfer from the TFTP server. The new file is placed into inactive firmware image. [Y, N]
- **Image Verify**—Initiate the verification of the integrity of firmware file held in unit. [1, 2]
- **Image Copy**—Initiate the copying of the active firmware into the inactive image. [Y, N]

- **Reboot Device**—Initiate rebooting the *transceiver*. This will interrupt data traffic through this unit, and the network if performed on an Access Point. Intended to be used to toggle between firmware images. [1, 2]

Upgrading the Firmware

NOTE: MDS iNET radios beginning with the serial numbers shown in Table 2-6 require a specific version of bootloader code to initialize the radio. Attempts to downgrade units to a firmware version earlier than the one listed will prevent the radio from initializing, and will require returning the unit to the factory for non-warranty service. The same data for iNET-II radios is shown in Table 2-7.

Additionally, radios that are part of a P21 Protected Network Station must not be downgraded to a firmware version prior to 5.4.3 (or to a version prior to listed in Table 2-6).

Table 2-6. iNET Serial Numbers and Code Revisions

Serial Number Range	Minimum Code Revision(s)
2598153 and later**	8.1.1
1882447 through 2598152**	6.9.1
1823400 through 1882446	6.7.0
1245286 through 1823399	5.5.0, 5.0.1, 4.8.0 or 3.5.1*
Prior	Any

* Refer to software release notes for additional information.

** Radios built and shipped from GE MDS starting from October 2014 may contain a hardware incompatible with older revisions.

Table 2-7. iNET-II Serial Numbers and Code Revisions

Serial Number Range	Minimum Code Revision(s)
2598153 and later**	8.1.1
1911387 through 2598152**	2.7.0
Prior	2.0.0

** Radios built and shipped from GE MDS starting from October 2014 may contain hardware incompatible with older revisions.

Firmware images are available free-of-charge at www.gemds.com.

NOTE: Starting in October 2014, iNET and iNET-II radios built may contain hardware that is incompatible with older revisions of firmware and cannot be downgraded. To see if a particular radio has the incompatible hardware, view the *Reprogramming Menu* (as seen in Figure 2-75 on Page 83). A string will be printed at the bottom of the page noting: **This hardware supports only builds >= 8.0.0**. If not, the radio may be downgraded one firmware tier (as noted by the above tables). Otherwise, downgrading is not allowed and attempting to downgrade below 8.1.1 will fail.

NOTE: MDS iNET firmware may *not* be installed in MDS iNET-II radios, or vice-versa.

To install firmware by TFTP, you will need:

- A PC with a TFTP server running.
- The IP address of the PC running the TFTP server.
- A valid firmware file

The IP address of the radio can be found under the Management Systems' **Configuration** menu. (See "Network Configuration Menu" on Page 27.)

A TFTP server is available on the GE MDS Web site at www.gemds.com.

NOTE: The iNET and the TFTP server must be on the same subnet.

TIP: If you do not know your computer's address on a Windows PC, you can use the **RUN** function from the **Start** menu and enter **winipcfg** or **ipconfig** to determine your local PC's IP address.

There are several alternatives to connecting the transceiver for firmware upgrade. Figure 2-76 and Figure 2-77 show two variations. It is essential all of the equipment be on the same subnet.

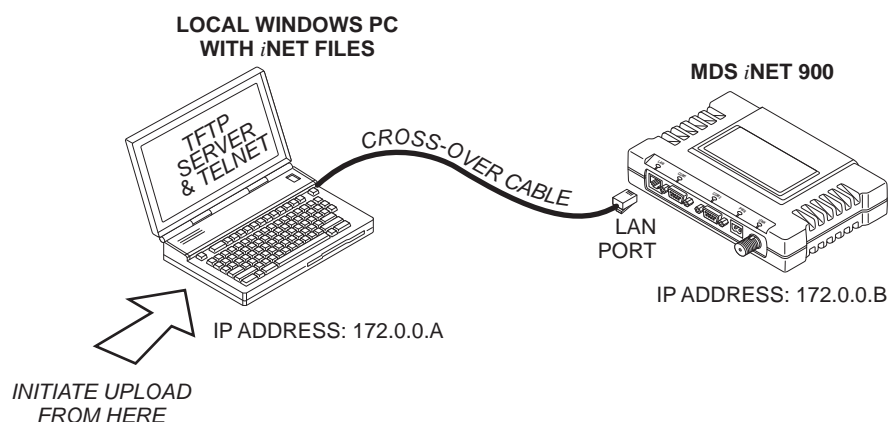


Figure 2-76. Firmware Upgrade Setup—Option 1
(TFTP Server and Firmware File on Same CPU)

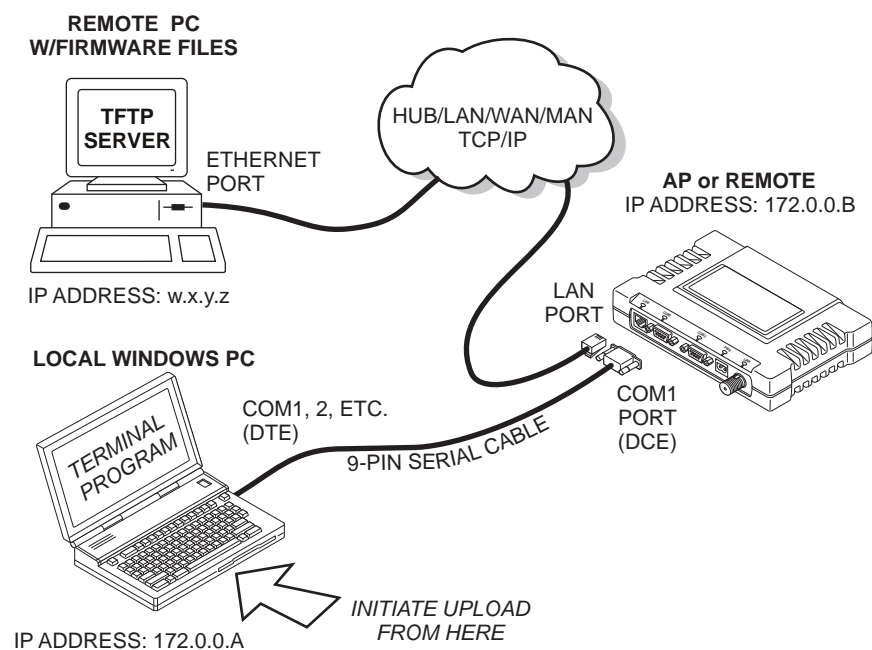


Figure 2-77. Firmware Upgrade Setup—Option 2
(TFTP Server and Firmware File on Remote Server)

NOTE: The LAN and COM1 ports share a common data channel when loading firmware over-the-air. Transferring the radio firmware image file (≈ 3 Mb), may take several minutes depending on traffic between the TFTP server and the transceiver.

Regardless of your connection to the transceiver, loading firmware/configuration files into the unit's flash-RAM is much slower than loading software onto a PC hard drive or RAM.

Upgrade Procedure

To load a new firmware file (**filename.ipk**) into the transceiver, use the following procedure:

1. Launch a TFTP server on a PC connected either directly or via a LAN to the Ethernet port (LAN) of the radio. Point the server towards the directory containing the firmware image file.
2. Connect to the Management System by whichever means is convenient: Browser or Telnet via the LAN, or Terminal emulator via the COM1 port.
3. Go to the Reprogramming Menu.
(Main Menu>>Maintenance/Tools Menu>>Reprogramming Menu)
4. Fill in the information for the:
 - **TFTP Host Address**—IP Address of server (host computer) running TFTP server.
 - **Filename**—Name of file (**filename.ipk**) to be pulled from the TFTP server holding the firmware file.

5. Pull the firmware file through the TFTP server into the transceiver.
(Main Menu>>Maintenance/Tools Menu>>Reprogramming Menu>>Retrieve File)

Status messages on the transfer are posted on the Management System screen.

NOTE: The new firmware image file that replaces the “Inactive Image” file will be automatically verified.

6. Reboot the transceiver.
Main Menu>>Maintenance/Tools Menu>>Reprogramming Menu>>Reboot Device

7. Test the transceiver for normal operation.

End of Procedure

NOTE: During a reprogramming session, functional operation and services will be limited. Allow the unit to finish the reprogramming session before using any management interfaces.

Error Messages During File Transfers

It is possible to encounter errors during a file transfer. In most cases errors can be quickly corrected by referring to Table 2-8.

Table 2-8. Common Errors During TFTP Transfer

Error Message	Likely Cause/Corrective Action
Invalid File Type	Indicates that the file is not a valid firmware file. Locate proper file and re-load.
File not found	Invalid or non-existent filename on TFTP server
Invalid file path	Invalid or non-existent file path to TFTP server

Table 2-8. Common Errors During TFTP Transfer

Error Message	Likely Cause/Corrective Action
Timeout	TFTP transfer time expired. Increase the timeout value.
Flash Error	Flash memory error. Contact factory for assistance.
Bad CRC	Cyclic Redundancy Check reporting a corrupted file. Attempt to re-load, or use a different file.
Version String Mismatch	Invalid file detected. Attempt to re-load, or use a different file.
Sending LCP Requests	The PPP server is querying for any clients that may need to connect.
Port not Enabled	The serial port is disabled.

2.9.2 Configuration Scripts Menu

A configuration script file contains all of the settable parameters of a radio that are accessible through the menu interface, with a few exceptions. A configuration script file is in plain text format and can be easily edited in a text program.

Configuration scripts can be helpful in several ways. Three common uses for them are:

- To save and restore known-good configuration files from your radios.
- To facilitate the configuration of a large number of radios.
- To provide troubleshooting information when you contact the factory for technical support.

How Configuration Files Work

When a configuration script file is downloaded to a radio (**Retrieve**), the radio executes the parameters as commands and takes the values contained in it. When a configuration script file is uploaded from the radio (**Send**) it contains the current values of the parameters that the radio is configured with. Figure 2-78 on Page 87 shows the Configuration Scripts Menu.

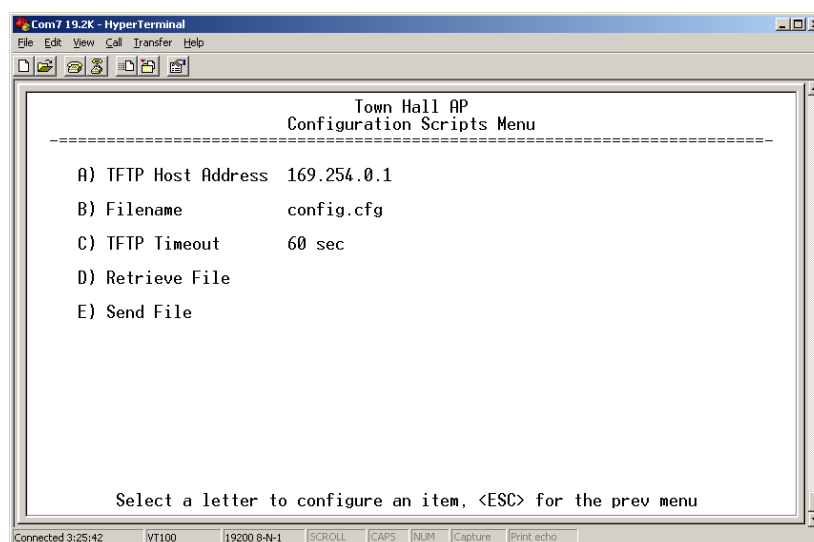


Figure 2-78. Configuration Scripts Menu

- **TFTP Host Address**—IP address of the computer on which the TFTP server resides. [Any valid IP address]
- **Filename**—Name of file containing this unit’s configuration profile that will be transferred to the TFTP server. The configuration information will be in a plain-text ASCII format. [Any 40-character alphanumeric string] May require a sub-directory, for example: `config\inet-config.txt`. (See “Configuration Scripts Menu” on Page 87 for more information.)

NOTE: The filename field is used to identify the desired incoming file and as the name of the file being exported to the TFTP server. Before exporting a unit’s configuration, you may want to name it in a way that reflects the radio’s services or other identification.

- **TFTP Timeout**—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the *transceiver* before suspending the file transfer. [10 to 120 seconds; 10]
- **Retrieve File**—Initiate the file transfer of the configuration file from TFTP server into the transceiver.
- **Send File**—Initiate the file transfer from the transceiver’s current configuration file to TFTP server.

NOTE: See “Upgrading the Firmware” on Page 84 for details on setting up the TFTP server.

Editing Configuration Files

Once a Remote unit’s operation is fine-tuned, use the “Configuration Scripts Menu” on Page 87 to save a copy of the configuration on a PC. Once the file is saved on the PC it can be used as a source to generate modified copies adjusted to match other devices. The configuration files can be modified using a text editor or an automated process. (These applications are not provided by GE MDS).

We recommend that you review and update the following parameters for each individual unit. Other parameters may also be changed as necessary. Each resulting file should be saved with a different name. We recommend using directories and file names that reflect the location of the unit to facilitate later identification.

Table 2-9. Common User-Alterable Parameters

Field	Comment	Range
IP Address	Unique for each individual radio	Any legal IP address
IP Gateway	May change for different groups or locations	Any legal IP address
Unit Name	Should reflect a specific device. This information will appear in Management System headings	Any 20-character alphanumeric string
Location	Used only as reference for network administration	Any 40-character alphanumeric string

Editing Rules

- You may include only parameters you want to change from the default value.
- Change only the parameter values.
- Capitalization counts in some field parameters. (Example: System Mode)
- Comment Fields
 - Edit, or delete anything on each line to the right of the comment delimiter, the semicolon (;).
 - Comments can be of any length, but must be on the same line as the parameter, or on a new line that begins with a semicolon character.
 - Comments after parameters in files exported from a transceiver do not need to be present in your customized files.
- Some fields are read-only. These are designated by “(RO)” in the configuration sample file.

2.9.3 Authorization Key Menu

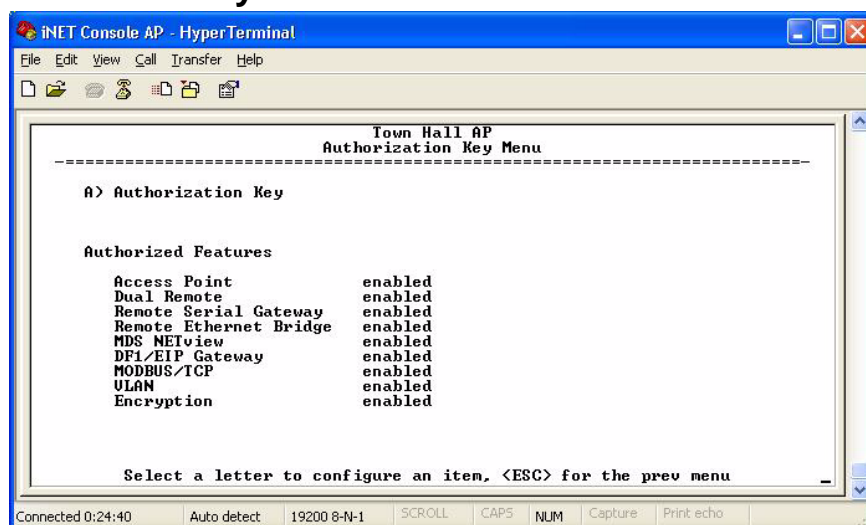


Figure 2-79. Authorization Key Menu
(iNET-II image shown; iNET omits Encryption option)

- **Authorization Key**—Initiate the entering of an Authorization Key into the transceiver's non-volatile memory.
- **Authorized Features**—List of authorized features available for use [**enabled**, **disabled**].

MDS iNET-II radios will show an additional selection called **Encryption** under Authorized Features.

Additionally, the user can enter an authcode directly from the login prompt by entering 'authcode' as the password. This will then display the radios's serial number and prompt the user for the authcode. To exit the authcode menu without entering an authcode, simply press the **Enter** key.

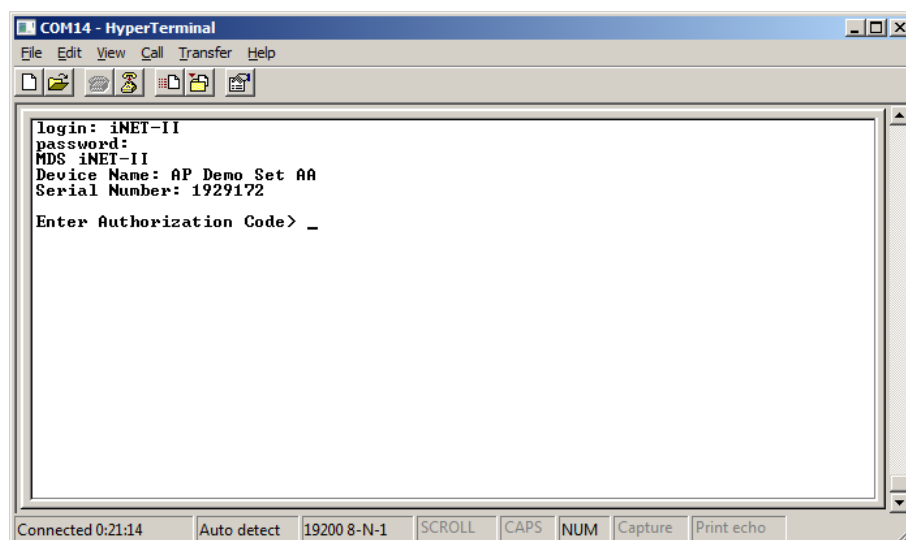


Figure 2-80. Login Prompt Authcode Entry

2.9.4 Change the Type of Remote

For iNET-900 units only enter the serial number of the unit to be changed in the **Auth Key** field to turn a Serial Gateway Remote into an Ethernet Bridge Remote, or vice-versa.

2.9.5 Auto-Upgrade/Remote-Reboot Menu

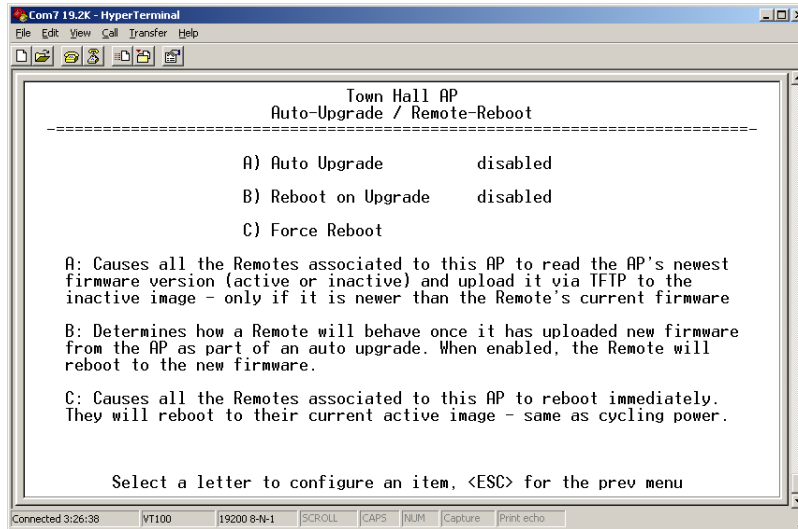


Figure 2-81. Auto-Upgrade / Remote Reboot Menu

- **Auto Upgrade**—Causes all of the Remotes associated to this AP to read the AP's newest firmware version (active or inactive) and upload it via TFTP to the inactive image, but only if it is newer than the Remote's current firmware.
- **Reboot on Upgrade**—Determines how a Remote will behave once it has uploaded new firmware from the AP as part of an auto-upgrade. When enabled, the Remote will reboot to the new firmware.
- **Force Reboot**—Causes all of the Remotes associated to this AP to reboot immediately. They will reboot to their current active image—the same as if the power were re-cycled.

NOTE: To use the Auto Upgrade/Reboot feature, both the AP and Remotes must already be running version 4.4.0 or newer firmware.

Exception: If the AP has already been upgraded to version 4.4.0 and the Remote is still at 3.5.0 or older, you can upgrade the Remote by using the AP as a file server. This method allows for only one remote to be upgraded at a time. Instructions for this method are given below.

Firmware Upgrade (with AP Acting as a TFTP Server)

An AP running firmware version 4.4.0 (or newer) may be used as a file server to upgrade Remotes running older firmware (3.5.0 or earlier). Follow the steps below to perform the upgrade:

1. At the Reprogramming Menu (Page 83), Enter the AP's IP Address in the TFTP Server field.
2. Enter **upgrade_from_ap.ipk** in the Filename field.

NOTE: The filename is case sensitive.

3. Perform the firmware download.

2.9.6 Radio Test Menu

Using this menu, you can manually key the radio transmitter to make measurements of antenna performance. (See "Antenna Aiming" on Page 115 for details.)

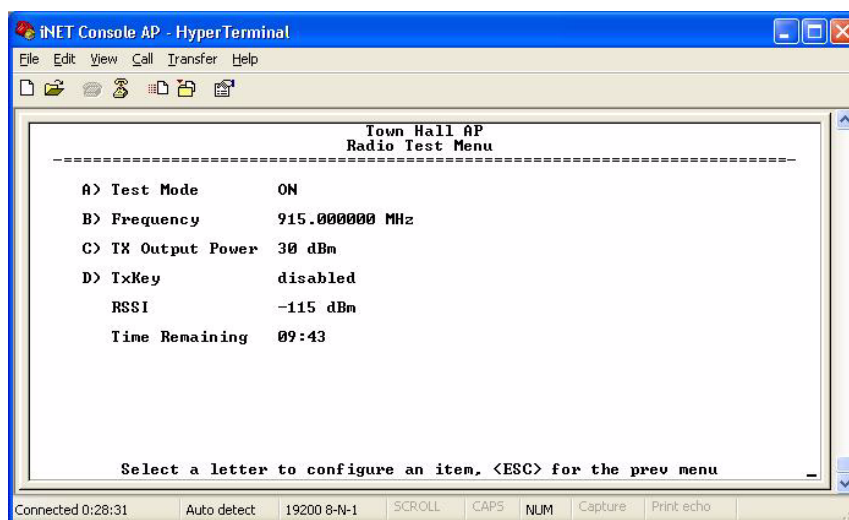


Figure 2-82. Radio Test Menu
(Shown with Test Mode set to ON)

NOTE : Use of the Test Mode will disrupt traffic through the radio. If the unit is an Access Point, it will disrupt traffic through the *entire* network.

Test Mode function is automatically limited to 10 minutes and *should only be used for brief measurement of transmit power*. It may also be manually reset to continue with the testing or turned off.

- **Test Mode**—Controls access to the transceiver's suite of tools. [ON, OFF; OFF]
- **Frequency**—Set radio operating frequency during the testing period to a single frequency. [902.5-927.5035 MHz (iNET), 902.8165-927.1870 MHz (iNET-II); 915.0000 MHz]
- **TX Output Power**—Temporarily overrides the power level setting in the Radio Configuration Menu. [20 to 30 dBm]
- **TxKey**—Manually key the radio transmitter for power measurements. [Enable, Disable; Disable]
- **RSSI**—Incoming received signal strength on frequency entered in the frequency parameter on this screen (–dBm). This RSSI measurement is updated more frequently than the RSSI by Zone display of the Performance Information menu. Note that for the MDS iNET, the RSSI is an average of the RSSI samples. The RSSI value is reset every time the radio returns to scanning mode.

2.9.7 Ping Utility Menu

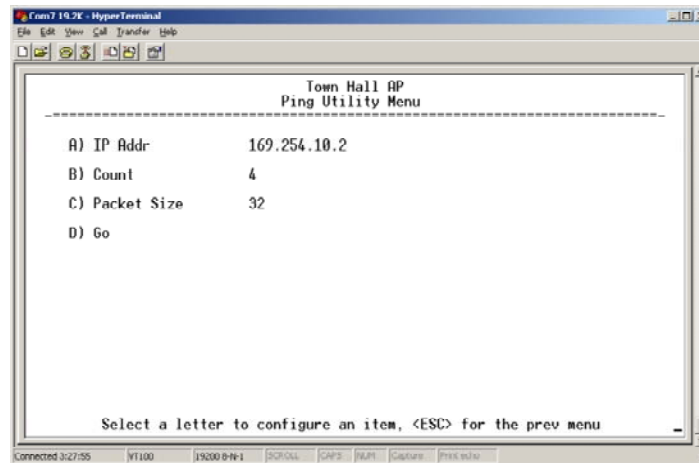


Figure 2-83. Ping Utility Menu

- **IP Addr**—Address to send a PING. [Any valid IP address]
- **Count**—Number of PING packets to be sent. [1 to 999999999; 4]
- **Packet Size**—Size of each PING data packet (bytes). [1 to 65507; 32]
- **Go**—Send PING packets to address shown on screen.

Screen will be replaced with detailed report of PING activity. Press any key after viewing the results to return to this menu. Press [Ctrl + C] to stop the pings and return to this menu.

2.9.8 Reset to Factory Defaults

NOTE: Use this procedure carefully. All parameters will be reset to factory defaults.

To reset all transceiver parameters back to the factory defaults, select the **Reset to Factory Defaults** option in the **Maintenance/Tools Menu**. The radio will then reboot into its defaulted state. This procedure *does not* reset the user-configured password. See “Password Reset to Factory Default” on Page 92.

This procedure is useful when several parameters have been modified, and there is no track of changes. It causes the transceiver to return to a known state.

Password Reset to Factory Default

Only use this procedure if you want to also reset the password to the factory default password. As part of the reset action, the transceiver’s password is reverted to the default value of **admin**. As a security measure, this event causes *all* radio parameters to return to the factory default settings, including zone skipping (as applicable), baud rate settings, network name, security phrase, and so on.

To achieve this, enter a special code (authorization key) provided by the factory in place of the password at the time of login.

2.9.9 Support Bundle

The Support Bundle Menu page provides an interface to download a Support Bundle file. The Support Bundle contains configuration, debugging, and diagnostic information that can be useful to the MDS Technical Services team in assisting with diagnosing problems with a unit or system.

The Support Bundle is a binary file and is encoded due to the proprietary nature of some of the content. The MDS Technical Services team is able to decode the file. The file can be downloaded using the standard file transfer techniques used for firmware, configuration files, and event logs.

NOTE: These support bundles are the same as if exporting an Event Log named **mds_eng.log** using the Event Log Menu see “Event Log Menu” on Page 71. This gives the user the opportunity to name the log for ease of identifying the radio.

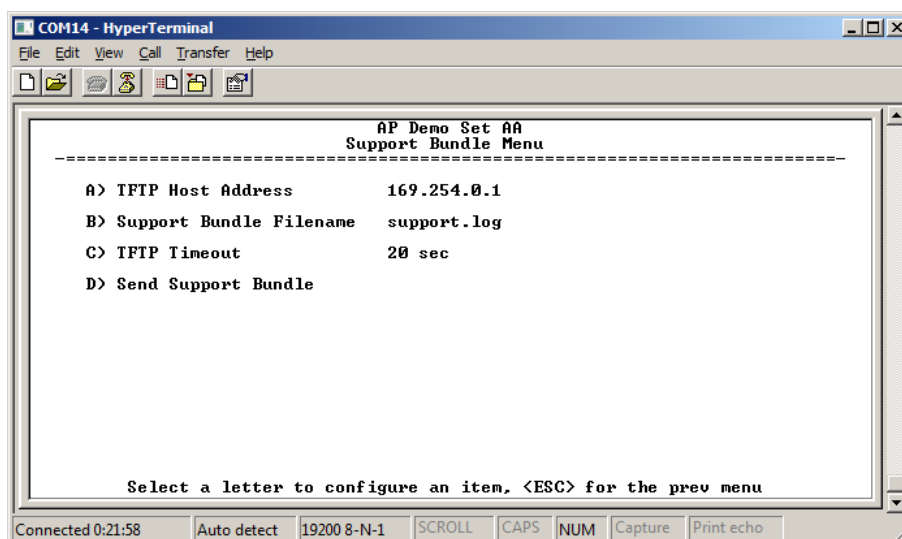


Figure 2-84. Support Bundle Menu

- **TFTP Host Address**—Address of the TFTP Server. [Any valid IP address]
- **Support Bundle Filename**—Name of the support bundle. [1-40 characters;support.log]
- **TFTP Timeout**—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the *transceiver* before canceling the file transfer. [2 to 60 seconds; 20]
- **Send Support Bundle**—Send the support bundle.

3.0 TROUBLESHOOTING

3.1 Introduction

Successful troubleshooting of a wireless system is not difficult, but requires a logical approach. It is best to begin troubleshooting at the Access Point unit, as the rest of the system depends on the Access Point for synchronization data. If the Access Point has problems, the operation of the entire wireless network will be affected.

When communication problems are found, it is good practice to begin by checking the simple things. Applying basic troubleshooting techniques in a logical progression can identify many problems.

3.1.1 Multiple Communication Layers

It is important to remember the operation of the network is built upon a radio communications link. On top of that are two data levels— wireless MAC, and the data layer. It is essential that the wireless aspect of the Access Point and the Remote units to be associated are operating properly before data-layer traffic will function.

3.1.2 Unit Configuration

There are over 50 user-configurable parameters in the Management System. Do not overlook the possibility that human error may be the cause of the problem. With so many possible parameters to look at and change, a parameter may be incorrectly set, and then what was changed is forgotten.

To help avoid these problems, we recommend creating an archive of the transceiver's profile when your installation is complete in a Configuration File. This file can be reloaded into the transceiver to restore the unit to the factory defaults or your unique profile. For details on creating and archiving Configuration Files, see "*Configuration Scripts Menu*" on Page 87.

3.1.3 Factory Assistance

If problems cannot be resolved using the guidance provided here, review the GE MDS website's technical support area for recent software/firmware updates, general troubleshooting help, and service information. Additional help is available through our Technical Services Department. (See "TECHNICAL ASSISTANCE" on the inside of the rear cover.)

3.2 Troubleshooting with LEDs

An important set of troubleshooting tools are the LED status indicators on the front panel of case. You should check them first whenever a problem is suspected. Table 3-1 on Page 95 provides suggestions for resolving common system difficulties using the LEDs, and Table 3-2 on Page 96 provides other simple techniques.

Table 3-1. Troubleshooting Using LEDs—Symptom-Based

Symptom	Problem/Recommended System Checks
PWR LED does not turn on	<ol style="list-style-type: none"> Voltage too low—Check for the proper supply voltage at the power connector. (10–30 Vdc) Indefinite Problem—Cycle the power and wait (\approx 30 seconds) for the unit to reboot. Then, recheck for normal operation.
LINK LED does not turn on	<ol style="list-style-type: none"> Network Name of Remote not identical to desired Access Point. Verify that the system has a unique Network Name. Not yet associated with an Access Point with the same Network Name. Check the “Status” of the unit’s process of associating with the Access Point. Use the Management System. Poor Antenna System. Check the antenna, feedline and connectors. Reflected power should be less than 10% of the forward power reading (SWR 2:1 or lower). Security Parameters do not match, preventing Remotes to join. Disable or correct these parameters.
PWR LED is blinking	<ol style="list-style-type: none"> Blinking indicates an alarm condition exists. View Current Alarms and Event Log and correct the problem if possible. (See “Using Logged Operation Events” on Page 99) Blinking will continue until the source of the alarm is corrected, for example, a valid IP address is entered, etc.
LAN LED does not turn on	<ol style="list-style-type: none"> Verify the Ethernet cable is connected at both ends. Verify that the appropriate type of Ethernet cable is used: straight-through, or crossover.
LAN LED lights, but turns off after some time	Verify traffic in LAN. Typically, the radio should not be placed in high traffic enterprise LANs, as it will not be able to pass this level of traffic. If needed, use routers to filter traffic.

3.3 Troubleshooting with the Menu System

If you have reviewed and tried the things mentioned in Table 3-1 and still have not resolved the problem, there are some additional tools and techniques that can be used. The radio’s embedded Management System is a good source of information that may be used remotely to provide preliminary diagnostic information, or may even provide a path to correcting the problem.

Table 3-2. Basic Troubleshooting Using the Management System

Symptom	Problem/Recommended System Checks
Remote does not associate; stays in HOPSYNC	<ol style="list-style-type: none"> Verify the AP has sufficiently large number in the “Max Remotes” parameter of the Network Configuration Menu. Verify the correct MAC address is listed in the “Approved Remotes List” or “Approved Access Points List” of the Security Configuration menu.
Serial data is slow with UDP multicast traffic	Change Beacon Period to FAST in the Radio Configuration Menu.
Cannot access the MS through COM1	<ol style="list-style-type: none"> Connect to unit via Telnet or Web browser Disable the serial mode for COM1 (Serial Gateway Configuration>>Com1 Serial Data Port>>Status>>Disabled) or, if you know the unit's data configuration: <ol style="list-style-type: none"> Connect to COM 1 via a terminal set to VT100 and the port's data baud rate. Type +++ Change the terminal's baud rate to match the transceiver's Console Baud Rate. Type +++
Display on terminal/Telnet screen garbled	Verify the terminal/terminal emulator or Telnet application is set to VT100
Cannot pass IP data to WAN.	<ol style="list-style-type: none"> Verify your IP settings. Use the PING command to test communication with the transceivers in the local radio system. If successful with local PING, attempt to PING an IP unit attached to a transceiver. If successful with the LAN PINGs, try connecting to a known unit in the WAN.
Wireless Retries too high.	<p>Possible Radio Frequency Interference—</p> <ol style="list-style-type: none"> If omnidirectional antennas are used, consider changing to directional antennas. This will often limit interference to and from other stations. Try skipping some zones where persistent interference is known or suspected. The installation of a filter in the antenna feedline may be necessary. Consult the factory for further assistance.
Password forgotten.	<ol style="list-style-type: none"> Connect to the transceiver using a terminal through the COM1 Port. Obtain a password-resetting Authorization Key from your factory representative. Enter the Authorization Key at the login prompt as a password.
Packet Repeat Mode troubles (extra characters in data, data not delivered)	Verify that all radios in the network have their Packet Redundancy Mode set to the same selection (Single Packet vs. Packet Repeat Mode).

The following is a summary of how several screens in the Management System can be used as diagnostic tools.

3.3.1 Starting Information Screen

(See “Starting Information Screen” on Page 22)

The Management System’s “homepage” provides some valuable bits of data. One of the most important is the “Device Status” field. This item will tell you if the unit is showing signs of life.

If the *Device Status* field says *Associated*, then look in the network areas beginning with network data statistics. If it displays some other message, such as *Scanning*, *Hop Sync* or *Alarmed*, you will need to determine why it is in this state.

The Scanning state indicates a Remote unit is looking for an Access Point beacon signal to lock onto. It should move to the Hop Sync and finally to the Associated state within less than a minute. If this Remote unit is not providing reliable service, look at the *Event Log* for signs of lost association with the Access Point or low signal alarms. Table 3-3 provides a description of the Device Status messages.

Table 3-3. Device Status¹

Scanning	The unit is looking for an Access Point beacon signal.
Hop Sync	The unit has found a valid beacon signal for its network and has changed its frequency hopping pattern to match that of the AP.
Connected	The unit has established a radio (RF) connection with the Access Point, but has not obtained cyber-security clearance to pass data.
Associated	This unit has successfully synchronized and is “associated” with an Access Point. This is the normal operating state.
Alarmed	The unit is has detected one or more alarms that have not been cleared.

1. Available in the *Starting Information Screen* or the *Wireless Network Status* at the Remotes.

If the Remote is in an “Alarmed” state, the unit may still be operational and associated. Look for the association state printed on the *Starting Information Screen* next to “Alarmed”. If it is, then look at the *Event Log* for possible clues.

If the unit is in an “Alarmed” state and not able to associate with an Access Point unit, then there may be problems with the wireless network layer. Call in a radio technician to deal with wireless issues. Refer the technician to the “Radio (RF) Measurements” on Page 114 for information on antenna system checks.

3.3.2 Packet Statistics Menu

(See “Packet Statistics Menu” on Page 74)

This screen provides detailed information on data exchanges between the unit being viewed and the network through the wireless and the Ethernet (data) layers. These include:

Wireless Packet Statistics

- Packets received
- Packets sent
- Bytes received
- Bytes sent
- Packets dropped
- Receive errors
- Retries
- Retry errors

Ethernet Packet Statistics

- Packets received
- Packets sent
- Bytes received
- Bytes sent
- Lost carrier detected
- Packets dropped
- Receive errors

The most significant fields are the *Packets dropped*, *Receive errors*, *Retries*, *Retry errors*, and *Lost carrier detected*. If the data values are more than 10% of their sent and received counterparts, or the *Lost carrier detected* value is greater than a few dozen, there may be trouble with radio-frequency interference or a radio link of marginal strength. Review the *RSSI by Zone Screen*’s values (page 71) for zones that are more than 2 dB (decibels) below the average level, and for signal level values that are likely to provide marginal service. For example, an average level is less than -85 dBm during normal conditions with a data rate of 256 kbps.

If the RSSI levels in each zone are within a few dB of each other, but less than -85 dBm, then a check should be made of the aiming of the antenna system and for a satisfactory SWR. Refer to “Radio (RF) Measurements” on Page 114 for information on antenna system checks.

NOTE: For a data rate of 512 kbps (1 Mbps for iNET-II), the average signal level should be -77 dBm or stronger with no interference.

3.3.3 Serial Port Statistics Menu

(See “Serial Data Statistics Menu” on Page 81)

This screen provides top-level information on data exchanges between the unit’s serial ports and the network through the wireless and the Ethernet (data) layers. These include the following items:

- Bytes In On Port
- Bytes In On Socket
- Bytes Out On Port
- Bytes Out On Socket

You can use this screen as an indicator of port activity at the data and IP levels.

3.3.4 Diagnostic Tools

(See “Maintenance” on Page 82)

The radio’s Maintenance/Tools menu contains two tools that are especially useful to network technicians—the Radio Test Menu and the Ping Utility. The Radio Test selection allows for testing RF operation, while the Ping Utility can be used to verify reachability to pieces of equipment connected to the radio network. This includes transceivers and user-supplied Ethernet devices.

3.4 Using Logged Operation Events

(See “Event Log Menu” on Page 71)

The transceiver’s microprocessor monitors many operational parameters and logs them as various classes of “events”. If the event is one that affects performance, it is an “alarm”. There are also normal or routine events such as those marking the rebooting of the system, implementation of parameter changes and external access to the Management System. Informational events are stored in temporary (RAM) memory that will be lost in the absence of primary power, and Alarms will be stored in permanent memory (Flash memory) until cleared by user request. Table 3-4 summarizes these classifications.

Table 3-4. Event Classifications

Level	Description/Impact	Storage
Informational	Normal operating activities	RAM
Minor	Does not affect unit operation	RAM
Major	Degraded unit performance but still capable of operation	RAM
Critical	Prevents the unit from operating	Flash Memory

These various events are stored in the transceiver’s “Event Log” and can be a valuable aid in troubleshooting unit problems or detecting attempts at breaching network security.

3.5 Alarm/Event Conditions

(See “View Current Alarms” on Page 73)

Most events, classified as “critical” or Alarms will make the PWR LED blink, and will inhibit normal operation of the transceiver. The LED blinks until the corrective action is completed.

Table 3-5. Alarm/Event Conditions (Alphabetical Order)

Alarm Condition Reported	Event Log Entry	SNMP Trap
EVENT_50_LIMIT*	Crossed 50% of Eth Port Rate Limit	rateLimit50(20)
EVENT_75_LIMIT*	Crossed 75% of Eth Port Rate Limit	rateLimit75(21)
EVENT_100_LIMIT*	Crossed 100% of Eth Port Rate Limit	rateLimit100(22)
EVENT_ADC	ADC output Railed	adcInput(3)
EVENT_BRIDGE	Network Interface Error	networkInterface(17)
EVENT_ETH_LINK_AP*	AP Ethernet Link Disconnected	apEthLinkLost(19)
EVENT_FLASH_TEST	Flash Test Failed	--
EVENT_FPGA	FPGA communication Failed	fpgaCommunication(2)
EVENT_FREQ_CAL	Frequency Not Calibrated	frequencyCal(7)
EVENT_INIT_ERR	Initialization Error	initializationError(18)
EVENT_IPADDR*	IP Address Invalid	ipAddressNotSet(4)
EVENT_IPMASK*	IP Mask Invalid	ipNetmaskNotSet(5)
EVENT_MAC	MAC communication Failed	macCommunication(1)

Table 3-5. Alarm/Event Conditions (Alphabetical Order)(Continued)

Alarm Condition Reported	Event Log Entry	SNMP Trap
EVENT_MACADDR	MAC Address Invalid	noMacAddress(6)
EVENT_NETNAME*	Netname Invalid	invalidNetname(12)
EVENT_NO_CHAN*	Using Channel hopping but no channels selected	NoChan(23)
EVENT_PLL_LOCK	PLL Not locked	pllLock(10)
EVENT_POWER_CAL	Power Calibrated/Not Calibrated	powerCal(8)
EVENT_POWER_HIGH	RF Power Control Saturated High	rfPowerHigh(13)
EVENT_POWER_LOW	RF Power Control Saturated Low	rfPowerLow(14)
EVENT_REDUNDANCY_SWITCH	Redundancy Switchover Set	redundancySwitch(24)
EVENT_RSSI*	RSSI Exceeds threshold	rssi(11)
EVENT_RSSI_CAL	RSSI Not Calibrated	rssiCal(9)
EVENT_SYSTEM_ERROR*	System Error Cleared; Please Reboot	systemError(16)

* Condition may be corrected and alarm cleared, by user.

3.6 Correcting Alarm Conditions

(See “View Event Log” on Page 73)

Table 3-6 provides insight on the causes of events that inhibit the unit from operating, and possible corrective actions. The Event Log Entry column shows the text that appears in the Description column on the **Event Log** screen.

Table 3-6. Correcting Alarm Conditions—Alphabetical Order

Event Log Entry	Generating Condition	Clearing Condition or Action
Ethernet Rate Above 50, 75, 100%	Data on the Ethernet port has reached the % value of the configured Ethernet Rate Limit.	Reduce traffic on network, unplug Ethernet cable from radio.
ADC Output Railed	The ADC always reads the same value (either high or low limit)	Contact factory Technical Services for assistance
AP Ethernet Link Disconnected	Monitor will check state of Ethernet link and set alarm if it finds the link down	Ethernet link is re-established
Channels Not Programmed	No channels programmed.	Configure channels.
Flash Test Failed	Internal check indicates corruption of Flash memory	Contact factory Technical Services for assistance
FPGA communication Failed	Communication lost to the FPGA	Contact factory Technical Services for assistance

Table 3-6. Correcting Alarm Conditions—Alphabetical Order(Continued)

Event Log Entry	Generating Condition	Clearing Condition or Action
Frequency Not Calibrated	Calibration Error	Contact factory Technical Services for assistance
Initialization Error	Unit fails to complete boot cycle	Contact factory Technical Services for assistance
IP Address Invalid	The IP address is either 0.0.0.0 or 127.0.0.1	Program IP address to something other than 0.0.0.0 or 127.0.0.1
IP Mask Invalid	IP Mask not configured properly	Set the IP Mask to a proper configuration
MAC Address Invalid	Invalid MAC address programmed	Contact factory Technical Services for assistance
MAC communication Failed	The monitor task reads the LinkStatus from the MAC every second. If the MAC does not reply 10 consecutive times (regardless of what the result is) the CPU assumes the transceiver has lost communication to the MAC.	Contact factory Technical Services for assistance
Network Interface Error	Unit does not recognize the LAN interface, when the Bridge fails to be initialized	Contact factory Technical Services for assistance
Netname Invalid	Network name is "Not Programmed"	Change Network Name to something other than "Not Programmed"
PLL Not locked	The FPGA reports a synthesizer out-of-lock condition when monitored by the CPU.	Contact factory Technical Services for assistance.
Power Not Calibrated	Power not calibrated	Contact factory Technical Services for assistance
Redundancy Switchover Set	Radio has been triggered to switchover to the other redundant radio.	Allow radio to switchover to other redundant radio.
RF Power Control Saturated High	Power control can no longer compensate and reaches the high rail	Contact factory Technical Services for assistance
RF Power Control Saturated Low	Power control can no longer compensate and reaches the low rail	Contact factory Technical Services for assistance
RSSI Below Threshold	The running-average RSSI level is weaker (more negative) than the user-defined value.	Check aiming of the directional antenna used at the Remote; or raise the threshold level to a stronger (less-negative) value.
RSSI Not Calibrated	RSSI not calibrated	Contact factory Technical Services for assistance
System Error, Please Reboot	Unit encounters something that causes a system error.	Reboot the radio. If condition continues after reboot, contact factory Technical Services.

3.7 Logged Events

(See “View Event Log” on Page 73)

The following events allow the transceiver to continue operation and do not make the PWR LED blink. Each is reported through an SNMP trap. The left hand column, “Event Log Entry” is what will be shown in the Event Log.

Table 3-7. Non-Critical Events—Alphabetical Order

Event Log Entry	Severity	Description
AP is Not Approved/No Longer Approved	MAJOR	May occur during the Scanning process at a remote. Indicates that the received beacon came from an AP which is not in the “Approved AP” list. This may be caused by some remotes hearing multiple AP's. This event is expected behavior.
Association Attempt Success/Failed	MAJOR	Self explanatory
Association Lost - AP Hop Parameter Changed	MINOR	Self explanatory
Association Lost - AP's Ethernet Link Down	MAJOR	Self explanatory
Association Lost - AP's Network Name Changed	MINOR	Self explanatory
Association Lost - Local Network Name Changed	MAJOR	Self explanatory
Association Lost/Established	MAJOR	Self explanatory
Auth Demo Mode Expired -- Rebooted Radio/Enabled	MAJOR	Self explanatory
Auth Key Entered - Key Valid/Key Invalid	MAJOR	Self explanatory
Auth Failed	MAJOR	AP or Remote using 802.1X Device Authentication. Logged when RADIUS authentication fails.
Bit Error Rate Below threshold/Above threshold	INFORMATIONAL	Self explanatory
Certificate Chain Verified/Invalid	CRITICAL	Self explanatory
Compression State Changed to Disabled/Enabled	MINOR	Self explanatory
Connection Established/Lost	MAJOR	Remote using 802.1X Device Authentication. Logged when the Remote and AP have established a radio link and the RADIUS authentication can begin to establish data link.
Connection Timer Expired	MINOR	Remote Prioritized AP Mode. If the Remote is associated but not to the highest priority AP, it disconnects when the configured Connection Time expires to find a higher-priority AP.
Current AP Dropped - Forced	INFORMATIONAL	Self explanatory

Table 3-7. Non-Critical Events—Alphabetical Order(Continued)

Event Log Entry	Severity	Description
Current AP Dropped - RSSI	INFORMATIONAL	Remote Mobility Mode. If AP's RSSI falls below the configured threshold, Remote will drop the current AP and begin scanning for an AP with a better signal.
Date/Time from Server	INFORMATIONAL	Self explanatory
Desired AP IP Addr Mismatch	INFORMATIONAL	Self explanatory
Encryption Changed to Enable/Disable	MINOR	Self explanatory
Endpoint Removed/Added	MAJOR	Self explanatory
Ethernet Port Enabled/Disabled	INFORMATIONAL	Self explanatory
Expected Sync Lost/Established	INFORMATIONAL	Self explanatory
FPGA Reset disable	INFORMATIONAL	Self explanatory
Hop Format/SkipZone Mismatch	INFORMATIONAL	Self explanatory
Hop Sync Lost/Established	INFORMATIONAL	Self explanatory
Hop Table Generated/Generation Failed	INFORMATIONAL	Self explanatory
HTTP Access Locked for 5 Min	MAJOR	Self explanatory
HTTP User Logged Out/Logged In	MAJOR	Self explanatory
IP Connectivity OK	MINOR	Self explanatory
Lack of Associated Remotes Within/Exceeds Threshold	MAJOR	Redundancy Event
Local Console Access Locked for 5 Min	MAJOR	Self explanatory
Local Console User Logged Out/Logged In	MAJOR	Self explanatory
Local IP Address Changed	MAJOR	Self explanatory
Log Cleared	INFORMATIONAL	Self explanatory
Loss of Association Within Threshold/Exceeds Threshold	MAJOR	Redundancy Event
MAC Decryption Failed/MAC Decryption OK	MINOR	A decryption error is logged when an encryption phrase mismatch has occurred. A mismatch is declared after five consecutive errors over a 40-second window. When the error has cleared, MAC DECRYPT OK will appear.

Table 3-7. Non-Critical Events—Alphabetical Order(Continued)

Event Log Entry	Severity	Description
MAC Param Changed Attempt Re-Assoc	MINOR	Caused by remotes running in auto data rate mode. Every time the link conditions cause a data rate change, the remote's MAC changes to the new rate and forwards a signal to the AP. This indicates link quality is changing and causing the data rate to adjust accordingly.
Max Beacon Wait Time Exceeded	MAJOR	Self explanatory
Num Channels Defined Does not Match	MAJOR	iNET with Channels hop format. Number of channels on AP does not equal number of channels on Remote.
Packet Receive Errors Within/Exceeds Threshold	MAJOR	Redundancy Event
Packet Retry Errors Within/Exceeds Threshold	MAJOR	Redundancy Event
Received Beacon - AP is Blacklisted	INFORMATIONAL	Self explanatory
Received Beacon - Netname Does Not Match	INFORMATIONAL	Self explanatory
Received Beacon - Valid/Errored	INFORMATIONAL	Self explanatory
Rem Ethernet Link Connected/Disconnected	MAJOR	Self explanatory
Remote Console Access Locked for 5 Min	MAJOR	Self explanatory
Remote Mode Switched: Serial to Eth/Eth to Serial	MAJOR	Self explanatory
Remote Removed/Added	MAJOR	AP Removed/Added a Remote from its database.
Remote User Logged Out/Logged In	MAJOR	Self explanatory
Reprogramming Complete	INFORMATIONAL	Self explanatory
Reprogramming Failed	MAJOR	Self explanatory
Reprogramming Started	INFORMATIONAL	Self explanatory
Route Add Failed	MINOR	Self explanatory
Route Delete Failed	MINOR	Self explanatory
Scanning Started	INFORMATIONAL	Self explanatory
SDB Read Error / Counter Error	MAJOR	AP's Remote database Error.
SNR Within threshold/Below threshold	INFORMATIONAL	Self explanatory
System Bootup (power on)	INFORMATIONAL	Self explanatory
TFTP Server Finish Xfer / Start Xfer	INFORMATIONAL	Self explanatory

Table 3-7. Non-Critical Events—Alphabetical Order(Continued)

Event Log Entry	Severity	Description
TFTP Server Xfer Failed	MINOR	Self explanatory
Unapproved AP Beacon Received	MINOR	Remote Approved Access Points List mode. Logged when scanning continues because the received AP beacon is not in the approved list.
User Selected Reboot	MAJOR	Self explanatory
x509 Certs Loaded/Failure	CRITICAL	Self explanatory

4.0 PLANNING A RADIO NETWORK

4.1 Installation Planning

This section provides tips for selecting an appropriate site, choosing an antenna system, and reducing the chance of harmful interference.

NOTE: To prevent moisture from entering the radio, do not mount the radio with the cable connectors pointing up. Also, dress all cables to prevent moisture from running along the cables and into the radio.

4.1.1 General Requirements

There are three main requirements for installing a transceiver—adequate and stable primary power, a good antenna system, and the correct interface between the transceiver and the data device. Figure 4-1 shows a typical Remote Gateway installation.

NOTE: The iNET network port supports 10BaseT connections, but does not support 100BaseT connections. This should not present a problem because most hubs/switches auto-switch between 10BaseT and 100BaseT connections. Confirm that your hub/switch is capable of auto-switching data rates.

To prevent Ethernet traffic from degrading iNET performance, place the iNET in a segment, or behind routers.

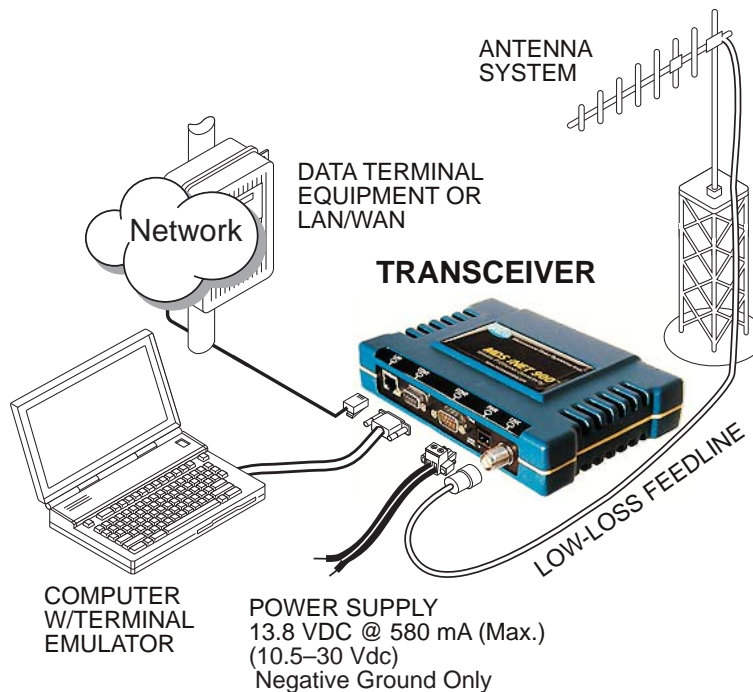


Figure 4-1. Typical Installation with a Tower-Mounted Antenna
(Connect user data equipment to any compatible LAN or COM Port)

Unit Dimensions

Figure 4-2 shows the dimensions of the transceiver case and its mounting holes, and Figure 4-3 on Page 108, the dimensions for mounting with factory-supplied brackets. If possible, choose a mounting location that provides easy access to the connectors on the end of the radio and an unobstructed view of the LED status indicators.

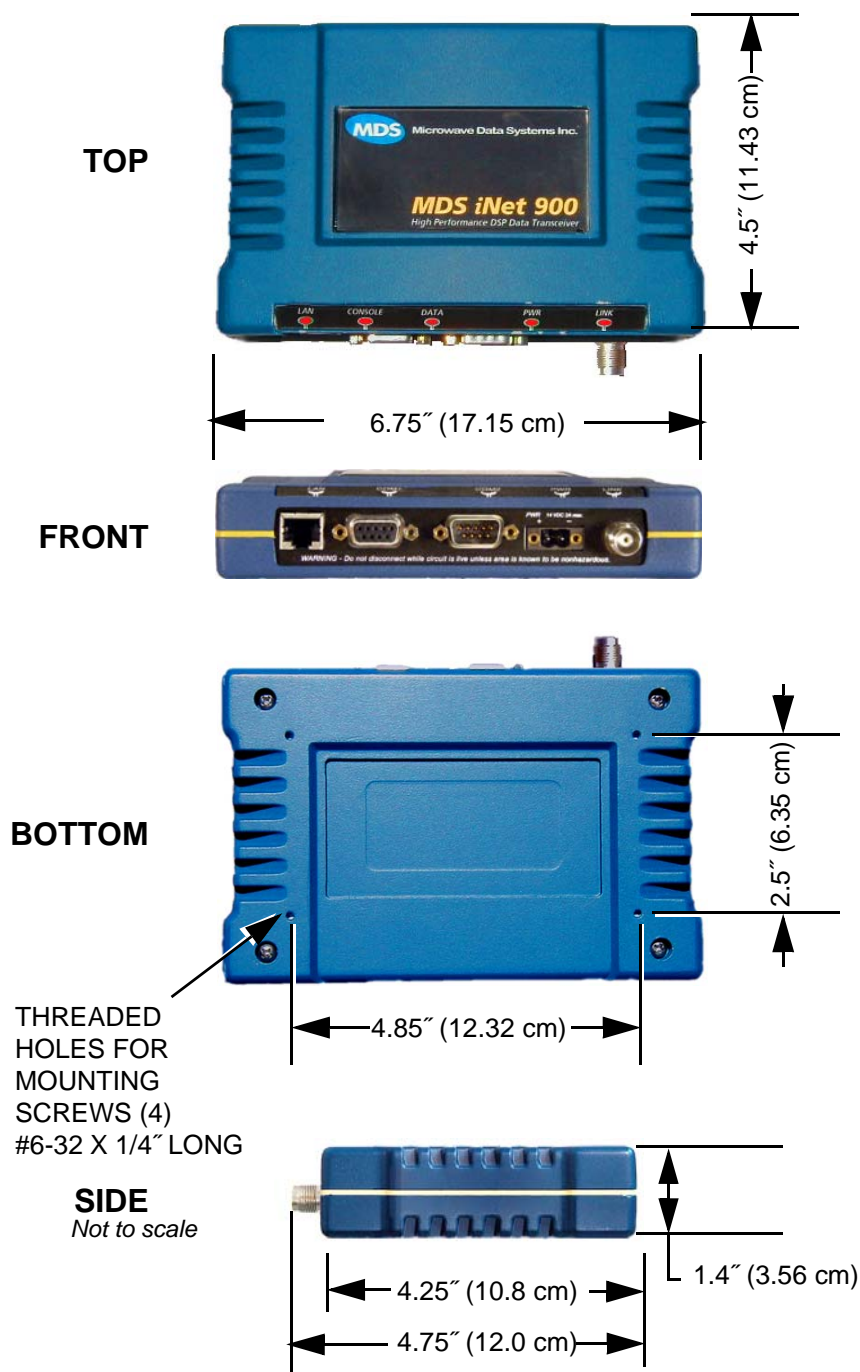


Figure 4-2. Transceiver Dimensions

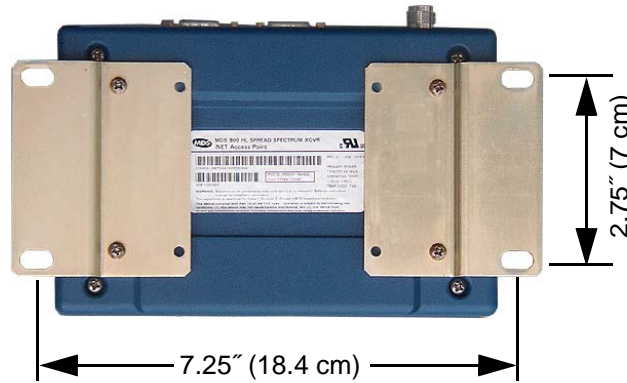
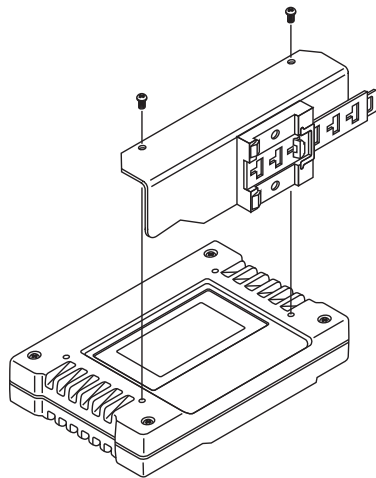


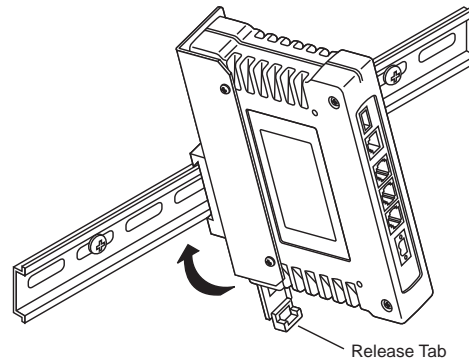
Figure 4-3. Mounting Bracket Dimensions

DIN Rail Mounting Option

The unit may also be mounted with an optional 35mm DIN Rail Mounting Bracket (Part No. 03-4125A04). Equipment cabinets and racks of recent design often employ this type of mounting. Once the DIN bracket is mounted to the iNET case, it allows for quick installation and removal of the radio without the need for tools of any kind. Figure 4-4 shows how the DIN Rail bracket attaches to the back of the unit's case, and how the entire unit attaches to the mounting rail.



Step 1: Attach the bracket using the two screws provided. (Attach to the end opposite the connectors.)



Step 2: Snap the assembly onto the DIN Rail. Removal is performed by pulling down on the release tab.

Figure 4-4. DIN Rail Mounting of GE MDS Equipment

4.1.2 Site Selection

Suitable sites should provide:

- Protection from direct weather exposure
- A source of adequate and stable primary power
- Suitable entrances for antenna, interface or other required cabling
- Antenna location that provides as unobstructed a transmission path as possible in the direction of the associated station(s)

These requirements can be quickly determined in most cases. A possible exception is the last item—verifying that an unobstructed transmission path exists. Radio signals travel primarily by line-of-sight, and obstructions between the sending and receiving stations will affect system performance. If you are not familiar with the effects of terrain and other obstructions on radio transmission, the discussion below will provide helpful background.

4.1.3 Equipment Grounding—Important

To minimize the chance of damage to the transceiver and connected equipment, a safety ground (NEC Class 2 compliant) is recommended which bonds the antenna system, transceiver, power supply, and connected data equipment to a *single-point* ground, keeping all ground leads as short as possible.

Normally, the transceiver is adequately grounded if the supplied flat mounting brackets are used to mount the radio to a well-grounded metal surface. If the transceiver is not mounted to a grounded surface, it is recommended that a safety ground wire be attached to one of the mounting brackets or a screw on the transceiver's case.

The use of a lightning protector is recommended where the antenna cable enters the building. Bond the protector to the tower ground, if possible.

4.1.4 Terrain and Signal Strength

While the license-free 900 MHz band offers many advantages for data transmission services, signal propagation is affected by attenuation from obstructions such as terrain, foliage or buildings in the transmission path.

A line-of-sight transmission path between the central transceiver and its associated remote site(s) is highly desirable and provides the most reliable communications link.

Much depends on the minimum signal strength that can be tolerated in a given system. Although the exact figure will differ from one system to another, a Received Signal Strength Indication (RSSI) of -77 dBm (-80 dBm for iNET-II) or stronger will provide acceptable performance in many systems. While the equipment will work at lower-strength signals, signals stronger than -77 dBm provide a “fade margin” of 15 dB to account for variations in signal strength that may occur from time-to-time. RSSI can be measured with a terminal connected to the COM1 Port or with a HTTP browser to the LAN (Ethernet) connector. (See “Antenna Aiming” on Page 115 for details.)

4.1.5 Antenna & Feedline Selection

NOTE: The transceiver is a Professional Installation radio system and must be installed by trained professional installers, or factory trained technicians.

This text that follows is designed to aid the professional installer in the proper methods of maintaining compliance with FCC Part 15 limits and the $+36$ dBm or 4 watts peak E.I.R.P limit.

Antennas

The equipment can be used with a number of antennas. The exact style used depends on the physical size and layout of a system. Contact your factory representative for specific recommendations on antenna types and hardware sources.

In general, an omnidirectional antenna (Figure 4-5) is used at the Access Point station site. This provides equal coverage to all of the Remote Gateway sites.

NOTE: Antenna polarization is important. If the wrong polarization is used, a signal reduction of 20 dB or more will result. Most systems using a gain-type omnidirectional antenna at the Access Point station employ vertical polarization of the signal; therefore, the remote antenna(s) must also be vertically polarized (elements oriented perpendicular to the horizon).

When required, horizontally polarized omnidirectional antennas are also available. Contact your factory representative for details.

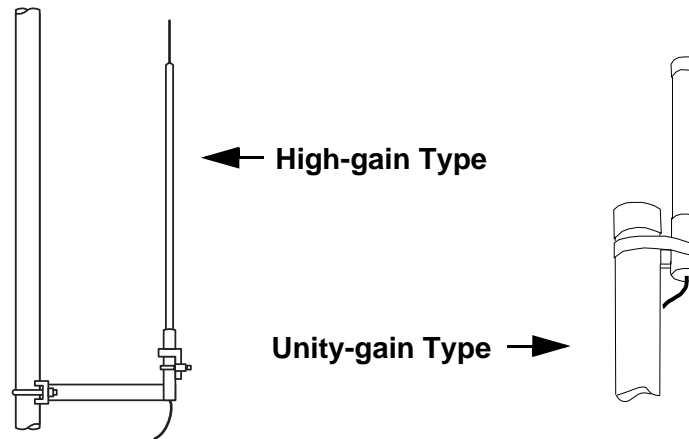


Figure 4-5. Typical Omnidirectional Antennas

At Remote Gateway sites and units in point-to-point LANs, a directional Yagi (Figure 4-6) antenna is generally recommended to minimize interference to and from other users. Antennas are available from a number of manufacturers.

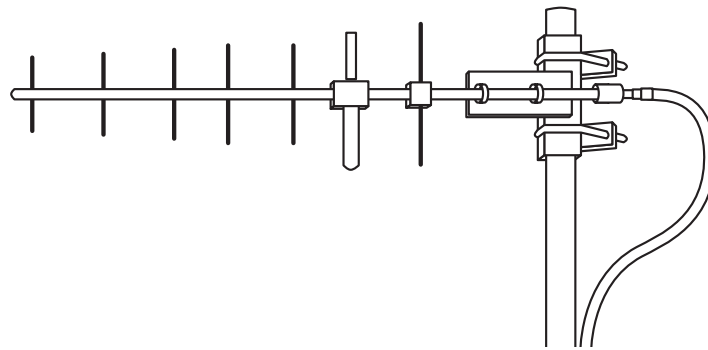


Figure 4-6. Typical Yagi Antenna (mounted to mast)

Feedlines

The choice of feedline used with the antenna should be carefully considered. Poor-quality coaxial cables should be avoided, as they will degrade system performance for both transmission and reception. The cable should be kept as short as possible to minimize signal loss.

For cable runs of less than 20 feet (6 meters), or for short range transmission, an inexpensive type such as Type RG-8A/U may be acceptable. Otherwise, we recommend using a low-loss cable type suited for 900 MHz, such as Helix[®].

Table 4-1 lists several types of popular feedlines and indicates the signal losses (in dB) that result when using various lengths of cable at 900 MHz. The choice of cable will depend on the required length, cost considerations, and the amount of signal loss that can be tolerated.

Table 4-1. Length vs. Loss in Coaxial Cables at 900 MHz

Cable Type	10 Feet (3.05 m)	50 Feet (15.24 m)	100 Feet (30.48 m)	500 Feet (152.4 m)
RG-214	.76 dB	3.8 dB	7.6 dB	Unacceptable Loss
LMR-400	0.39 dB	1.95 dB	3.90 dB	Unacceptable Loss
1/2 inch HELIAX	0.23 dB	1.15 dB	2.29 dB	11.45 dB
7/8 inch HELIAX	0.13 dB	0.64 dB	1.28 dB	6.40 dB
1-1/4 inch HELIAX	0.10 dB	0.48 dB	0.95 dB	4.75 dB
1-5/8 inch HELIAX	0.08 dB	0.40 dB	0.80 dB	4.00 dB

The tables below outline the minimum lengths of RG-214 coaxial cable that must be used with common GE MDS omnidirectional antennas in order to maintain compliance with FCC maximum limit of +36 dBi. If other coaxial cable is used, the appropriate changes in loss figures must be made.

NOTE: The authority to operate the transceiver in the USA may be void if antennas other than those approved by the FCC are used. Contact your factory representative for additional antenna information.

Table 4-2. Feedline Length vs. Antenna Gain*

(Required for Regulatory compliance)

Antenna Gain (dBd)	Antenna Gain (dBi)	Minimum Feedline Length (Loss in dB)	EIRP Level @ Min. Length	Maxrad Antenna Part No.
Unity (0 dB)	2.15 dBi	No minimum length	+32.15 dBm	Omni #MFB900
3 dBd	5.15 dBi	No minimum length	+35.15 dBm	Omni # MFB900
5 dBd	7.15 dBi	3.1 meters (1.2 dB)	+35.95 dBm	Omni # MFB900
6 dBd	8.15 dBi	9.1 meters (2.2 dB)	+35.95 dBm	Yagi # BMOY8903
9.2 dBd	11.34 dBi	25 meters (5.34 dB)	+36.00 dBm	Yagi OGB9-915

*Refer to Table 4-3 for allowable power settings of the transceiver for each antenna type.

NOTE: There is no minimum feedline length required when a 6 dBi gain or less antenna is used, as the EIRP will never exceed 36 dBm which is the maximum allowed, per FCC rules. The transceiver's RF output power may only be adjusted by the manufacturer or its sub-contracted Professional Installer.

The MDS iNET-II Transceiver is factory set to +29 dBm power output to maintain compliance with the FCC's Digital Transmission System (DTS) Part 15 rules. These rules limit power to a maximum of 8 dBm/3 kHz, thus the iNET-II Transceiver is factory set to +29 dBm. When calculating maximum transceiver power output for iNET-II installations, use +29 dBm if antenna gain is 6 dBi or less. See "How Much Output Power Can be Used?" on Page 112 for power control of higher gain antennas.

4.1.6 How Much Output Power Can be Used?

The transceiver is normally supplied from the factory set for a nominal +30 dBm (+29 dBm for iNET-II) RF power output setting; this is the maximum transmitter output power allowed under FCC rules. The power must be *decreased* from this level if the antenna system gain exceeds 6 dBi. The allowable level is dependent on the antenna gain, feedline loss, and the transmitter output power setting.

NOTE: In some countries, the maximum allowable RF output may be limited to less than the figures referenced here. Be sure to check for and comply with the requirements for your area.

4.1.7 Conducting a Site Survey

If you are in doubt about the suitability of the radio sites in your system, it is best to evaluate them before a permanent installation is underway. This can be done with an on-the-air test (preferred method); or indirectly, using path-study software.

An on-the-air test is preferred because it allows you to see firsthand the factors involved at an installation site and to directly observe the quality of system operation. Even if a computer path study was conducted earlier, this test should be done to verify the predicted results.

The test can be performed by first installing a radio and antenna at the proposed Access Point (AP) station site (one-per-system). Then visit the Remote site(s) with another transceiver (programmed as a remote) and a hand-held antenna. (A PC with a network adapter can be connected to each radio in the network to simulate data during this test using the PING command.)

With the hand-held antenna positioned near the proposed mounting spot, a technician can check for synchronization with the Access Point station (shown by a lit LINK LED on the front panel) and measure the reported RSSI value. (See “Antenna Aiming” on Page 115 for details.) If adequate signal strength cannot be obtained, it may be necessary to mount the station antennas higher, use higher gain antennas, select a different site or consider installing a repeater station. To prepare the equipment for an on-the-air test, follow the general installation procedures given in this guide and become familiar with the operating instructions found in “Embedded Management System” on Page 14.

4.1.8 A Word About Radio Interference

The transceiver shares the radio-frequency spectrum with other 900 MHz services and other Part 15 (unlicensed) devices in the USA. As such, near 100% error-free communications may not be achieved in a given location, and some level of interference should be expected. However, the radio’s flexible design and hopping techniques should allow adequate performance as long as care is taken in choosing station location, configuration of radio parameters and software/protocol techniques.

In general, keep the following points in mind when setting up your communications network.

- Systems installed in rural areas are least likely to encounter interference; those in suburban and urban environments are more likely to be affected by other devices operating in the license-free frequency band and by adjacent licensed services.
- Use a directional antenna at remote sites whenever possible. Although these antennas may be more costly than omnidirectional types, they confine the transmission and reception pattern to a comparatively narrow lobe, that minimizes interference to (and from) stations located outside the pattern.
- If interference is suspected from a nearby licensed system (such as a paging transmitter), it may be helpful to use horizontal polarization of all antennas in the network. Because most other services use vertical polarization in this band, an additional 20 dB of attenuation to interference can be achieved by using horizontal polarization. Another approach is to use a bandpass filter to attenuate all signals outside the 900 MHz band.
- Multiple Access Point units can co-exist in proximity to each other with only very minor interference. Each network name has a different hop pattern. (See “Protected Network Operation using Multiple

Access Points” on Page 9.) Additional isolation can be achieved by using separate directional antennas with as much vertical or horizontal separation as is practical.

- If constant interference is present in a particular frequency zone (collection of 8 RF channels), it may be necessary to “skip” that zone from the radio’s hopping pattern. The radio includes built-in software to help users identify and remove blocked frequency zones from its hopping pattern. See Page 44 for more information on Skip Zones.
- If interference problems persist even after skipping some zones, try reducing the length of data streams. Groups of short data streams have a better chance of getting through in the presence of interference than do long streams.
- The power output of all radios in a system should be set for the lowest level necessary for reliable communications. This lessens the chance of causing unnecessary interference to nearby systems.

If you are not familiar with these interference-control techniques, contact your factory representative for more information.

Calculating System Gain

To determine the maximum allowable power setting of the radio, perform the following steps:

1. Determine the antenna system gain by subtracting the feedline loss (in dB) from the antenna gain (in dBi). For example, if the antenna gain is 9.5 dBi, and the feedline loss is 1.5 dB, the antenna system gain would be 8 dB. (If the antenna system gain is 6 dB or less, no power adjustment is required.)
2. Subtract the antenna system gain from 36 dBm (the maximum allowable EIRP). The result indicates the maximum transmitter power (in dBm) allowed under the rules. In the example above, this is 28 dBm.
3. If the maximum transmitter power allowed is less than 30 dBm, set the power to the desired level using the Management System.
(Main Menu>>Radio Configuration>>RF Output Power Setpoint)

For convenience, Table 4-3 lists several antenna system gains and shows the maximum allowable power setting of the radio. Note that a gain of 6 dB or less entitles you to operate the radio at full power output –30 dBm (28.7 dBm for iNET-II).

Table 4-3. Antenna System Gain vs. Power Output Setting

Antenna System Gain (Antenna Gain in dBi* minus Feedline Loss in dB†)	Maximum Power Setting (PWR command) iNET Radio	Maximum Power Setting (PWR command) iNET-II Radio	EIRP (in dBm)
Omni 6 (or less)	30	28	36
Omni 11.14	24	23	36

* Most antenna manufacturers rate antenna gain in dBd in their literature. To convert to dBi, add 2.15 dB.

† Feedline loss varies by cable type and length. To determine the loss for common lengths of feedline, see Table 4-1 on Page 111.

For assistance in the conversion of dBm to Watts, see “dBm-Watts-Volts Conversion Chart” on Page 117.

4.1.9 Notes on Using 28 VDC Power Supplies

Common 28 Vdc supplies are often high-current power supplies designed primarily to charge battery banks. The radio can be operated from these supplies, providing there are no transients on the leads as power is applied to the radio. Transients can be created that rise above 30 Vdc to a voltage that exceeds the primary voltage rating of the radio and can destroy its voltage regulators and other components. It is important to keep this potential hazard in mind when designing 28 Vdc power supply connections for the radio.

- Use a two-conductor cable to power to the radio. Then the currents in the positive and negative wires are equal and opposite, causing their magnetic fields to cancel. The result is no net inductance in the connection to cause voltage overshoot.
- Do not connect a radio to a power supply that is already powered up, unless necessary (that is, when connecting a radio to a battery bank and charger). When power is applied by switching on a power supply, the rise time of the supply is too slow to cause overshoot.
- Typically, there are multiple return paths for the negative side of the power supply, through the coaxial cable shield and the chassis, for example. Any imbalance in the currents in the power cable results in voltage overshoot, so this should be minimized during initial power-up if the supply cannot be turned off.
- Add a 1 to 2 Ω , 2 Watt resistor in series with the positive lead. This greatly limits voltage overshoot. Since these radios draw very little current in receive mode, and transmit only briefly, there is little loss in power efficiency. In transmit, the voltage drop is minimal and has no effect.
- Minimize the length of the power cabling, within reason.
- When power is applied from a power source having a relatively high (1 or 2 Ω) source impedance, or from a power source without a large amount of output capacitance, no overshoot occurs. Therefore, use a power supply that is rated appropriately for the radio if possible—avoid using power supplies that far exceed the radio's current requirements.

Direct any questions you have about interfacing to GE MDS radios to the Technical Services Department, using the information provided at the back of this guide.

4.2 Radio (RF) Measurements

There are several measurements that are a good practice to perform during the initial installation. They will confirm proper operation of the unit and if they are recorded, serve as a benchmark in troubleshooting should difficulties appear in the future. These measurements are:

- Transmitter Power Output
- Antenna System SWR (Standing-Wave Ratio)
- Antenna Direction Optimization

These procedures may interrupt traffic through an established network and should only be performed by a skilled radio-technician in cooperation with the network manager.

4.2.1 Antenna System SWR and Transmitter Power Output

Introduction

A proper impedance match between the transceiver and the antenna system is important. It ensures the maximum signal transfer between the radio and antenna. The impedance match can be checked indirectly by measuring the SWR (standing-wave ratio) of the antenna system. If the results are normal, record them for comparison for use during future routine preventative maintenance. Abnormal readings indicate a possible trouble with the antenna or the transmission line that will need to be corrected.

The SWR of the antenna system should be checked before the radio is put into regular service. For accurate readings, a wattmeter suited to 1000 MHz measurements is required. One unit meeting this criteria is the Bird Model 43™ directional wattmeter with a 801-1 or other appropriate element installed.

The reflected power should be less than 10% of the forward power ($\approx 2:1$ SWR). Higher readings usually indicate problems with the antenna, feedline or coaxial connectors.

If the reflected power is more than 10%, check the feedline, antenna and its connectors for damage.

Record the current transmitter power output level, and then set it to 30 dBm for the duration of the test to provide an adequate signal level for the directional wattmeter.

Procedure

1. Place a directional wattmeter between the ANTENNA connector and the antenna system.
2. Place the transceiver into the Radio Test Mode using the menu sequence below:
(Main Menu>>Maintenance/Tools Menu>>Radio Test>>Test Mode>>Y>>ON)

NOTE: The Test Mode has a 10-minute timer, after which it will return the radio to normal operation. The Radio Test Mode can be terminated manually by selecting **OFF** on the menu or temporarily disconnecting the radio's DC power.

3. Set the transmit power to 30 dBm. (This setting does not affect the output level during normal operation—only during Test Mode.)
(Main Menu>>Maintenance/Tools Menu>>Radio Test>>Test Mode>>Tx Power Output)
4. Key the transmitter.
(Main Menu>>Maintenance/Tools Menu>>Radio Test>>Test Mode>>TxKey>> Enable)
Use the PC's spacebar to key and unkey the transmitter ON and OFF. (Enable/Disable)
5. Measure the forward and reflected power into the antenna system and calculate the SWR and power output level. The output should agree with the programmed value.
(Main Menu>>Radio Configuration>>RF Power Output)
6. Turn off Radio Test Mode at the Access Point and Remote.
(Main Menu>>Maintenance/Tools Menu>>Radio Test>>Test Mode>>Disable)

End of procedure

4.2.2 Antenna Aiming

Introduction

The radio network integrity depends, in a large part, on stable radio signal levels being received at each end of a data link. In general, signal levels stronger than -77 dBm (-80 dBm for iNET-II) provides the basis for reliable communication that includes a 15 dB fade margin. As the distance between the Access Point and Remotes increases, the influence of terrain, foliage and man-made obstructions become more influential and the use of directional antennas at Remote locations becomes necessary. Directional antennas usually require some fine-tuning of their bearing to optimize the received signal strength. The transceiver has a built-in received signal strength indicator (RSSI) that can be used to tell you when the antenna is in a position that provides the optimum received signal.

RSSI measurements and Wireless Packet Statistics are based on multiple samples over a period of several seconds. The average of these measurements will be displayed by the Management System.

The measurement and antenna alignment process will usually take 10 or more minutes at each radio unit.

The path to the Management System menu item is shown in bold text below each step of the procedure.

Procedure

1. Verify the Remote transceiver is associated with an Access Point unit by observing the condition of the LINK LED (**LINK LED = On or Blinking**). This indicates that you have an adequate signal level for the measurements and it is safe to proceed.

2. View and record the *Wireless Packets Dropped* and *Received Error* rates.
(Main Menu>>Performance Information>>Packet Statistics>>Wireless Packet Statistics)

This information will be used later.

3. Clear the *Wireless Packets Statistics* history.

(Main Menu>>Performance Information>>Packet Statistics>>Wireless Packet Statistics>>Clear Wireless Stats)\

4. Read the RSSI level at the Remote.
(Main Menu>>Performance Information>>RSSI by Zone)

5. Optimize RSSI (less negative is better) by slowly adjusting the direction of the antenna.

Watch the RSSI indication for several seconds after making each adjustment so that the RSSI accurately reflects any change in the link signal strength.

6. View the *Wireless Packets Dropped* and *Received Error* rates at the point of maximum RSSI level. They should be the same or lower than the previous reading.

(Main Menu>>Performance Information>>Packet Statistics>>Wireless Packet Statistics)

If the RSSI peak results in an increase in the *Wireless Packets Dropped* and *Received Error*, the antenna may be aimed at an undesired signal source. Try a different antenna orientation.

End of procedure

4.3 dBm-Watts-Volts Conversion Chart

Table 4-4 is provided as a convenience for determining the equivalent voltage or wattage of an RF power expressed in dBm.

Table 4-4. dBm-Watts-Volts Conversion—for 50 Ohm Systems

dBm	V	Po	dBm	V	Po	dBm	mV	Po	dBm	μV	Po
+53	100.0	200W	0	.225	1.0mW	-49	0.80		-98	2.9	
+50	70.7	100W	-1	.200	.80mW	-50	0.71	.01μW	-99	2.51	
+49	64.0	80W	-2	.180	.64mW	-51	0.64		-100	2.25	.1pW
+48	58.0	64W	-3	.160	.50mW	-52	0.57		-101	2.0	
+47	50.0	50W	-4	.141	.40mW	-53	0.50		-102	1.8	
+46	44.5	40W	-5	.125	.32mW	-54	0.45		-103	1.6	
+45	40.0	32W	-6	.115	.25mW	-55	0.40		-104	1.41	
+44	32.5	25W	-7	.100	.20mW	-56	0.351		-105	1.27	
+43	32.0	20W	-8	.090	.16mW	-57	0.32		-106	1.18	
+42	28.0	16W	-9	.080	.125mW	-58	0.286				
+41	26.2	12.5W	-10	.071	.10mW	-59	0.251				
+40	22.5	10W	-11	.064		-60	0.225	.001μW			
+39	20.0	8W	-12	.058		-61	0.200		-107	1000	
+38	18.0	6.4W	-13	.050		-62	0.180		-108	900	
+37	16.0	5W	-14	.045		-63	0.160		-109	800	
+36	14.1	4W	-15	.040		-64	0.141		-110	710	.01pW
+35	12.5	3.2W	-16	.0355					-111	640	
+34	11.5	2.5W							-112	580	
+33	10.0	2W							-113	500	
+32	9.0	1.6W							-114	450	
+31	8.0	1.25W							-115	400	
+30	7.10	1.0W							-116	355	
+29	6.40	800mW							-117	325	
+28	5.80	640mW							-118	285	
+27	5.00	500mW							-119	251	
+26	4.45	400mW							-120	225	.001pW
+25	4.00	320mW							-121	200	
+24	3.55	250mW							-122	180	
+23	3.20	200mW							-123	160	
+22	2.80	160mW							-124	141	
+21	2.52	125mW							-125	128	
+20	2.25	100mW							-126	117	
+19	2.00	80mW							-127	100	
+18	1.80	64mW							-128	90	
+17	1.60	50mW							-129	80	.1fW
+16	1.41	40mW							-130	71	
+15	1.25	32mW							-131	61	
+14	1.15	25mW							-132	58	
+13	1.00	20mW							-133	50	
+12	.90	16mW							-134	45	
+11	.80	12.5mW							-135	40	
+10	.71	10mW							-136	35	
+9	.64	8mW							-137	33	
+8	.58	6.4mW							-138	29	
+7	.500	5mW							-139	25	
+6	.445	4mW							-140	23	.01fW
+5	.400	3.2mW									
+4	.355	2.5mW									
+3	.320	2.0mW									
+2	.280	1.6mW									
+1	.252	1.25mW									

4.4 Performance Notes

The following is a list of points that are useful for understanding the performance of the radio in your installation.

4.4.1 Wireless Bridge

The transceiver acts as a bridge. If any radio in your network is connected to a large LAN, such as may be found in a large office complex, there may be undesired multicast/broadcast traffic over the air. As a bridge, the radios transmit this type of frame.

The radio goes through a listening and learning period at start-up before it will send any packets over either of its ports. This is about 10 seconds after the CPU's operating system has finished its boot cycle.

The bridge code in the transceiver operates and makes decisions about packet forwarding just like any other bridge. The bridge code builds a list of source MAC addresses that it has seen on each of its ports. There are a few general rules that are followed when a packet is received on any port:

- If the destination address is a multicast or broadcast address, forward the packet to all remotes.
- If the destination address is not known, forward the packet to all remotes.
- If the destination address is known, forward the packet to the port that the destination is known to be on (usually the RF port).
- The bridge code uses Spanning Tree Protocol (STP) to prevent loops from being created when connecting bridges in parallel. For example, connecting two remotes to the same wired LAN could create a loop if STP was not used. Every bridge running STP sends out Bridge Protocol Data Units (BPDUs) at regular intervals so that the spanning tree can be built and maintained. BPDUs are 60-byte multicast Ethernet frames.

4.4.2 Distance-Throughput Relationship

Distance affects throughput. Because of timers and other components of the protocol, there is a practical distance limit of 30 miles (48 km) for reliable operation. After this, although data still flows, the throughput will begin to drop and latency will increase, due to additional retries between the radios. Packets may start to be dropped. Some applications may tolerate this; others may not. Repeater stations may be used to extend the range.

4.4.3 Data Latency—TCP versus UDP Mode

The latency of data passing through a network will depend on user data message length, the overall level of traffic on the network, and the quality of the radio path.

Under ideal conditions—low traffic and good RF signal path—the latency for units operating in the TCP mode, will typically be around 5 ms in each direction. However, when UDP multicast traffic is transported, the outbound packet latency (from AP to remote) is dependent on the beacon period.

UDP multicast packet latency can be minimized by setting the **Beacon Period** to **Fast** (52 ms). Changing beacon rate to **Fast** will result in an average latency of 31 ms, assuming outbound packets wait for a beacon transmission 50% of the time (26ms) plus the normal packet latency (5 ms).

4.4.4 Data Compression

Enabling this option uses an LZO compression algorithm for over-the-air data. Varying levels of data reduction are achieved depending on the nature of the data. Text files are typically the most compressible, whereas binary files are the least compressible. On average, a 30% increase in throughput can be achieved with compression enabled.

Compression is used on data packets of 100 bytes or more, including Ethernet, IP, and TCP/UDP headers.

4.4.5 Packets-per-Second (PPS)

The iNET-II radio has a limit of approximately 140 PPS (70 PPS in iNET). Consider this restriction when planning your network, especially when smaller packets are expected to make up the majority of the traffic as is the case with VoIP (Voice over IP).

4.4.6 Station-to-Station Traffic

When sending frames from an endpoint connected to one transceiver to *another* endpoint with a different transceiver, the throughput will be halved at best. This is because all frames must go through the AP and thus are transmitted twice over the same radio system. Therefore, in the previous 100-byte UDP example, the number of over-the-air bytes will be 380 bytes (190 bytes x 2) if the frame has to go station-to-station.

4.4.7 Interference has a Direct Correlation to Throughput

Interference could be caused by other radios at the same site, in nearby locations, or by high power transmitters such as paging systems.

4.4.8 Maximizing Throughput

Here are some suggestion on things to try that may maximize throughput:

1. *AP Only*: Increment the **Dwell Time** to the maximum of 262.1 ms. This lowers the overhead since it will stay longer on a channel. The down side is that if a particular channel is interfered with it will take longer to hop to another channel.
(Main Menu>>Radio Configuration>>Dwell Time)
2. *AP Only*: Change the **Beacon Period** to **Normal** (508 ms). This will also reduce the overhead of beacons sent out. On the down side, association time may be a little longer.
(Main Menu>>Radio Configuration>>Beacon Period)
3. Change the **Fragmentation Threshold** to the maximum of 1600. Longer packets will be sent over the air reducing overhead. On the other hand, if a packet is corrupted it will take longer to be retransmitted.
(Main Menu>>Radio Configuration>>Fragmentation Threshold)
4. Increase the **RTS Threshold** to 1600. RTS mechanism is used to reserve a time slot if packets exceed this number. On the other hand, a hidden-node might interfere more often than if RTS was not used.
(Main Menu>>Radio Configuration>>RTS Threshold)

Decreasing the **RTS Threshold**, to the 100 to 200 range, may improve throughput on a busy network. It will add small packets, but reduce collisions (and resulting re-tries) of large packets.
(Main Menu>>Radio Configuration>>RTS Threshold)

5. Activate compression on the Radio Configuration Menu (**Compression enabled**).
6. Use the **Performance Information Menu** to check the packets received by zone. (Remotes Only: **Main Menu>>Performance Information>>Packet Statistics>>Packets Received by Zone**)

Readings should be close in value. A significantly lower value (2% reduction) probably indicates interference. Performance can be improved by blocking the affected zones at the Access Point. (**Main Menu>>Radio Configuration>>Skip Zone Option**)
7. Use the **Performance Information Menu** to check for errors, retries and dropped packets. Do the same with Ethernet traffic.

With weak signals, interference, or hidden nodes, the optimal performance may be lower due to collisions and retries.

4.4.9 Placing an iNET Radio Behind a Firewall

iNET-II and iNET radios use the port numbers listed below. If you place the radio behind a firewall, make sure these port numbers are included in the allowed list:

- SSH:22<- Management
- TELNET:23<- Management
- SMTP:25<- DF1
- TFTP:69<- Reprogramming
- HTTP:80<- Management
- NTP:123<- Time server
- SNMP:161<- Management
- SNMP-TRAP:162<- Event management via traps
- HTTPS:443<- Management
- SYSLOG:514<- Event management via remote syslog server

These well-known port numbers follow the recommendation of IANA. For more information, go to <http://www.iana.org/assignments/port-numbers>.

4.5 SNMPv3 Notes

4.5.1 Overview

The transceiver's SNMP Agent supports SNMP version 3 (SNMPv3). The SNMPv3 protocol introduces Authentication (MD5/SHA-1), Encryption (DES), the USM User Table, and View-Based Access (Refer to RFC2574 for full details). The SNMP Agent has limited SNMPv3 support in the following areas:

- Both MD5 and SHA-1 Authentication for SNMPv3 are supported. To choose between the two different authentication protocols, choose the corresponding account which is described in the section on page 120.
- Limited USM User Table Manipulation. The SNMP Agent starts with nine default accounts. iNET does not support adding SNMPv3 accounts manually.

New views cannot be configured on the SNMP Agent. Views will be inherited for new accounts from the account that was cloned.

The SNMP Agent uses one password pair (Authentication / Privacy) for all accounts. This means that when the passwords change for one user, they change for all users.

SNMPv3 Accounts

The following default accounts are available for the SNMP Agent:

enc_mdsadmin—Read/write account using MD5 Authentication and Encryption.

auth_mdsadmin—Read/write account using MD5 Authentication.

enc_mdsviewer—Read only account using MD5 Authentication and Encryption.

auth_mdsviewer—Read only account using MD5 Authentication.

def_mdsviewer—Read only account with no Authentication or Encryption.

sha1_enc_mdsadmin—Read/write account using SHA-1 Authentication and Encryption.

sha1_auth_mdadmin—Read/write account using SHA-1 Authentication.

sha1_enc_mdsvviewer—Read only account using SHA-1 Authentication and Encryption.

sha1_auth_mdsvviewer—Read only account using SHA-1 Authentication.

Context Names

The following Context Names are used (please refer to RFC2574 for full details):

Admin accounts: **context_a** / Viewer accounts: **context_v**

All accounts share the same default passwords:

Authentication default password: **MDSAuthPwd** / Privacy default password: **MDSPrivPwd**

Passwords can be changed either locally (via the console) or from an SNMP Manager, depending on how the Agent is configured. If passwords are configured and managed locally, they are non-volatile and will survive a power-cycle. If passwords are configured from an SNMP manager, they will be reset to whatever has been stored for local management on power-cycle.

This behavior was chosen based on RFC specifications. The SNMP Manager and Agent don't exchange passwords, but actually exchange *keys* based on passwords. If the Manager changes the Agent's password the Agent doesn't know the new password; just the new key. In this case, only the Manager knows the new password. This could cause problems if the Manager loses the password. If that happens, the Agent becomes unmanageable. Resetting the Agent's passwords (and therefore keys) to what is stored in flash memory upon power-cycle prevents the serious problem of losing the Agent's passwords.

If passwords are managed locally, they can be changed on the Agent (via the console). Any attempts to change the passwords for the Agent via an SNMP Manager will fail when the Agent is in this mode. Locally defined passwords will survive a power-cycle.

In either case, the SNMP Manager needs to know the initial passwords that are being used in order to talk to the Agent. If the Agent's passwords are configured via the Manager, then they can be changed from the Manager. If the passwords are managed locally, then the Manager must be re-configured with any password changes in order to continue to talk to the Agent.

Password-Mode Management Changes

When the password management mode is changed, the active passwords used by the Agent may also change. Some common scenarios are discussed below:

Common Scenarios

- Passwords are currently being handled by the Manager. The assigned passwords are **Microwave** (Auth), and **Rochester** (Priv). Configuration is changed to manage the passwords locally. The passwords stored on the radio were Fairport (Auth), and Churchville (Priv) (If local passwords have *never* been used, then MDSAuthPwd and MDSPrivPwd will be used). These passwords will now be used by the Agent to re-generate keys. The Manager will need to know these passwords in order to talk to the Agent.
- Passwords are currently being managed locally. The local passwords are **Fairport** (Auth) and **Churchville** (Priv). Configuration is changed to handle the passwords from the Manager. The same passwords will continue to be used, but now the Manager can change them.
- Passwords are currently being managed locally. The local passwords are **Fairport** (Auth) and **Churchville** (Priv). Passwords are changed to **Brighton** (Auth) and **Perinton** (Priv). The Agent will immediately generate new keys based on these passwords and start using them. The Manager will have to be re-configured to use these new passwords.
- Passwords are currently being managed locally. The local passwords are **Fairport** (Auth) and **Churchville** (Priv). Configuration is changed to handle the passwords from the Manager. The Manager changes the passwords to **Brighton** (Auth) and **Perinton** (Priv). The radio is then rebooted. After a power-cycle, the radio will use the passwords stored in flash, which are **Fairport** (Auth) and **Churchville** (Priv). The Manager will have to be re-configured to use these new passwords.

Table 4-5. SNMP Traps (Sorted by Code)

SNMP Trap	Severity	Description
systemBoot(33)	CRITICAL	SNR Within threshold/Below threshold
systemReboot(34)	MAJOR	Telnet User Logged Out/Logged In
startScan(35)	INFORMATIONAL	Reprogramming Started
rxBeaconErrored(36)	INFORMATIONAL	Received Beacon - Netname Does Not Match
rxBeaconWrongNetworkName(37)	INFORMATIONAL	Received Beacon - AP is Blacklisted
rxBeaconFromBlacklistAP(38)	INFORMATIONAL	Max Beacon Wait Time Exceeded
expectedSync(39)	INFORMATIONAL	Expected Sync Lost/Established
hopSync(40)	INFORMATIONAL	Hop Sync Lost/Established
hopTableWrite(41)	INFORMATIONAL	Hop Table Generated/Generation Failed
snr(42)	INFORMATIONAL	Scanning Started
ber(43)	INFORMATIONAL	Bit Error Rate Below threshold/Above threshold
associated(44)	MAJOR	Association Lost/Established
apParmChange(45)	MINOR	Association Lost - AP Hop Parameter Changed
reprogStarted(46)	INFORMATIONAL	Reprogramming Failed
reprogComplete(47)	INFORMATIONAL	Rem Ethernet Link Connected/Disconnected
reprogFailed(48)	MAJOR	Reprogramming Complete
remoteConsoleLogin(49)	MAJOR	Remote Console User Logged Out/Logged In
httpLogin(50)	MAJOR	HTTP User Logged Out/Logged In
hopFormatSkipZoneMismatch(51)	INFORMATIONAL	Hop Format/SkipZone Mismatch
desiredAPIPMismatch(52)	INFORMATIONAL	Desired AP IP Addr Mismatch
eventLogCleared(53)	INFORMATIONAL	Log Cleared
authDemoMode(54)	MAJOR	Auth Demo Mode Expired -- Rebooted Radio/Enabled
keyEntered(55)	MAJOR	Auth Key Entered - Key Valid/Key Invalid
apEthLinkDown(56)	MAJOR	Association Lost - AP's Ethernet Link Down
noBeacons(57)	MAJOR	MAC Param Changed
apNotApproved(58)	MAJOR	Current AP No Longer Approved
netnameChanged(59)	MAJOR	Association Lost - Local Network Name Changed
ipAddrChanged(60)	MAJOR	Association Lost - Local IP Address Changed
assocTryFail(61)	MAJOR	Association Attempt Success/Failed
remEthLinkLost(62)	MAJOR	Received Beacon - Valid/Errored
localConsoleLogin(63)	MAJOR	Local Console User Logged Out/Logged In
localConsoleLockdown(64)	MAJOR	Local Console Access Locked for 5 Min
remoteConsoleLockdown(65)	MAJOR	Remote Console Locked for 5 Min
httpLockdown(66)	MAJOR	HTTP Access Locked for 5 Min
eventRemote(67)	MAJOR	Remote added/removed from internal database
eventEndpoint(68)	MAJOR	Endpoint added/removed from internal database

Table 4-5. SNMP Traps (Sorted by Code)(Continued)

SNMP Trap	Severity	Description
routeAdded(69)	MINOR	Radio attempted but failed to add a route to its internal routing table
routeDeleted(70)	MINOR	Radio attempted but failed to delete a route from its internal routing table
sinRemSwitch(71)	MAJOR	Remote mode was switched (serial to ethernet, ethernet to serial)
ChanCnt(72)	MAJOR	Number of channels defined does not match (Channel 130 only)
tftpConnection(74)	INFORMATIONAL	TFTP Server on AP started or finished a transfer
apNetNameChanged(75)	MINOR	Remote lost association due to a change in the AP's netname
ipConnectivityOK(76)	MINOR	Radio is associated AND 1) has an IP address statically defined, OR 2) received an IP address via DHCP
compressionChanged(77)	MINOR	Compression state has changed (enabled, disabled)
macDecryptError(78)	MINOR	MAC has received a packet that it could not decrypt
lanPortStatus(79)	MINOR	Ethernet port has changed (enabled, disabled)
macParamChanged(80)	MINOR	MAC parameter change that causes reassociation
tftpConnFailed(81)	MINOR	TFTP server on AP failed to transfer
sdbError(82)	MAJOR	AP encountered an internal database error
encryptionChanged(83)	MINOR	Over the Air Encryption enabled or disabled
mobileAPDrop(85)	INFORMATIONAL	Current AP dropped due to RSSI
forceMobileAPDrop(86)	INFORMATIONAL	Forced current AP to drop
redundancyLossAssoc(87)	MAJOR	Loss of Association Exceeded Threshold
redundancyLackRemotes(88)	MAJOR	Lack of Associated Remotes Exceeded Threshold
redundancyRetryErr(89)	MAJOR	Packet Retry Errors Exceeded Threshold
redundancyRecvErr(90)	MAJOR	Packet Receive Errors Exceeded Threshold
connExpire(92)	MINOR	Time before Remote moves to the next AP in the Approved AP List
unapprovedBeacon(93)	MINOR	Remote received a beacon from an unapproved AP
conn(94)	MAJOR	Over-the-Air Authentication Established/Lost
authentication(95)	MAJOR	Over-the-Air Authentication failed
fpgaReset(97)	INFORMATIONAL	Turn off/on FPGA logging
certVerify(98)	CRITICAL	X.509 Certificate is loaded or failed to load
certChainVerify(99)	CRITICAL	Certificate Chain validation verified or invalid
timeFromServer(100)	INFORMATIONAL	Date and Time received from Server

5.0 TECHNICAL REFERENCE

5.1 Data Interface Connectors

Three data interface connectors are provided on the face of the transceiver. The first, the LAN Port, is an RJ-45 connector. The other two use two DB-9 interface connectors that use the RS-232 (EIA-232) signaling standard. Note that the connector for COM1 Port is DCE (Female DB-9) and the COM2 Port is DTE (male DB-9).



The transceiver meets U.S.A.'s FCC Part 15, Class A limits when used with shielded data cables.

5.1.1 LAN Port

The transceiver's LAN Port is used to connect the radio to an Ethernet network. The transceiver provides a data link to an Internet Protocol-based (IP) network via the Access Point station. Each radio in the network must have a unique IP address for the network to function properly.

- To connect a PC directly to the radio's LAN port, an RJ-45 to RJ-45 cross-over cable is required.
- To connect the radio to a Ethernet hub or bridge, use a straight-through cable.

The connector uses the standard Ethernet RJ-45 cables and wiring. For custom-made cables, use the pinout information in Figure 5-1 and Table 5-1.

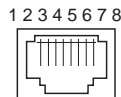


Figure 5-1. LAN Port (RJ-45) Pinout
(Viewed from the outside of the unit)

Table 5-1. LAN Port (IP/Ethernet)

Pin	Functions	Ref.
1	Transmit Data (TX)	High
2	Transmit Data (TX)	Low
3	Receive Data (RX)	High
4	Unused	
5	Unused	
6	Receive Data (RX)	Low
7	Unused	
8	Unused	

5.1.2 COM1 Port

To connect a PC to the transceiver's COM1 port use a DB-9M to DB-9F "straight-through" cable. These cables are available commercially, or may be constructed using the pinout information in Figure 5-2 and Table 5-2.

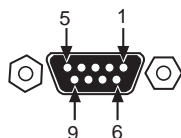


Figure 5-2. COM1 Port (DCE)
(Viewed from the outside of the unit.)

Table 5-2. COM1 Port Pinout, DB-9F/RS-232 Interface

Pin	Functions	DCE
1	Unused	
2	Receive Data (RXD)	<—[Out
3	Transmit Data (TXD)	—>[In
4	Unused	
5	Signal Ground (GND)	
6–9	Unused	

5.1.3 COM2 Port

To connect a PC to the transceiver's COM2 port use a DB-9F to DB-9M null modem "crossover" cable. These cables are available commercially, or may be constructed using the pinout information in Figure 5-3 and Table 5-3.

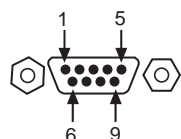


Figure 5-3. COM2 Port (DTE)
Viewed from the outside of the radio

Table 5-3. COM2 Port, DB-9M/EIA-232 Interface

Pin	Functions	DTE
1	Data Carrier Detect (DCD)	In]<—
2	Receive Data (RXD)	In]<—
3	Transmit Data (TXD)	Out]—>
4	Data Terminal Ready (DTR)	Out]—>
5	Signal Ground (GND)	
6	Data Set Ready (DSR)	In]<—
7	Request-to-Send (RTS)	Out]—>
8	Clear-to-Send (CTS)	In]<—
9	Unused	

5.2 Fuse Replacement

An internal fuse protects the transceiver from over-current conditions or an internal component failure. It should not be replaced until you are certain you are in a safe (non-flammable) environment.

1. Disconnect the primary power source and all other connections to the unit.
2. Place the radio on its back and remove the four Phillips screws on the bottom cover.
3. Carefully separate the top and bottom covers. There is a flat ribbon cable between the top cover's LEDs and the unit motherboard. You do not need to disconnect the ribbon cable.
4. Locate the fuse and fuse holder between the COM1 port and the power connector. See Figure 5-4 for details.
5. Loosen the fuse from the holder using a very small screwdriver. Use a small pair of needle-nose pliers to pull the fuse straight up and remove it.
6. Using an Ohmmeter, or other continuity tester, verify the fuse is blown.
7. Install a new fuse by reversing the process.
Littelfuse P/N: 0454002; 452 Series, 2 Amp SMF Slo-Blo
GE MDS P/N: 29-1784A03
8. Install the covers and check the transceiver for proper operation.

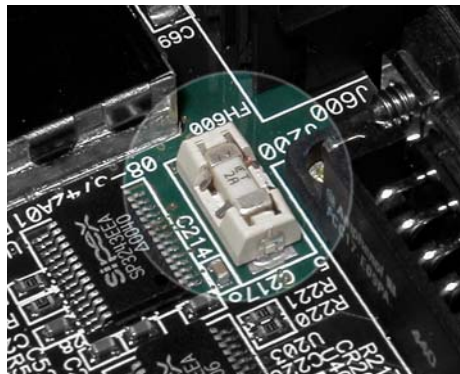


Figure 5-4.
Internal Fuse Location

5.3 Technical Specifications

GENERAL

Temperature Range:	–30° C to +60° C (–22° F to 140° F)
Humidity:	95% at +40° C (104° F); non-condensing
Primary Power:	10–30 Vdc (13.8 Vdc Nominal)
External Power Supply Options:	110–120/210–220 Vac
Supply Current (typical):	(9 Watts Maximum @ 1 Watt RF Output)
Transmit:	7 watts (10.5–24 Vdc) 9 watts (24.5–30 Vdc)
Receive:	2.8 watts (10.5–24 Vdc) 3.5 watts (24.5–30 Vdc)
MTBF (Reliability):	Consult factory for on-file data

Size (Excluding mtg. hardware): 1.25" x 6.75" x 4.5" (H x W x D)
3.15 x 17.15 x 11.43 cm

Mounting w/Optional Hardware:

- DIN Rail
- Flat surface mounting brackets
- 19" rack (1U high)

Weight: 908 g / 2 lb

Case: Cast Aluminum

Boot Time: ≈ 30 sec

Time Required to Associate
with Access Point: ≈ 20 sec

APPROVALS/HOMOLOGATION

- FCC Part 15.247
iNET FCC identifier: E5MDS-NH900
iNET-II FCC identifier: E5MDS-INETII
- Industry Canada RSS-210
iNET certification no.: 3738A 12098
iNET-II certification no.: 3738A-INETII
- UL/CSA Class 1, Div. 2; Groups A, B, C and D hazardous locations
- Complies with the following IEEE Standard: 1613™-2003 Communications Networking Devices in Electric Power Substations classifications:
4.1.1 Environmental Class B
4.1.2 Environmental Storage Class A
7.12 Device Performance Class 1
- Contact factory for information on availability and governmental approvals in other countries

MANAGEMENT

- HTTP, HTTPS (Embedded Web server)
- Telnet, SSH, COM1 serial port (Text-based menu)
- SNMP v1/v2/v3
- SYSLOG
- GE MDS PulseNET

DATA CHARACTERISTICS

PORTS:

Ethernet:

Interface Connectors: RJ-45 Standard
Data Rate: 10BaseT (10 Mbps)

Serial (2 Ports):

Signaling Standard: EIA-232/V.24
Interface Connectors: DB-9
Interface: COM1: DCE / COM2: DTE
Data Rate: 1200–115,200 bps
asynchronous

Data Latency: < 10 ms typical

Byte Formats: 7 or 8-bit; even, odd, or no-parity; 1 or 2 stop bits

OPERATING MODES:

- Configurable as Access Point or Remote Station

PROTOCOLS:

- Wireless: CSMA/CA (Collision Avoidance)
- Ethernet: IEEE 802.3, Ethernet II, Spanning Tree (Bridging), IGMP
- TCP/IP: DHCP, ICMP, UDP, TCP, ARP, Multicast, SNMP, TFTP
- Serial: PPP, Encapsulation over IP (tunneling) for serial async multidrop protocols including Modbus, DNP.3, DF1, BSAP
- Special: Allen-Bradley EtherNet/IP* - Modbus/TCP (optional)

CYBER SECURITY

Cyber Security,
Level 1 (iNET-II only):

- AES-128 encryption (optional)

Cyber Security,
Level 2:

- RC4-128 encryption (iNET only)
 - Automatic rotating key algorithm
 - Authentication: 802.1X, EAP/TLS, PKI, PAP, CHAP
 - Management: SSL, SSH, HTTPS
 - Approved AP/Remotes list (local authentication)
 - Failed login lockdown
 - 900 MHz operation and proprietary data framing

RADIO CHARACTERISTICS

GENERAL:

Frequency Range:	902–928 MHz ISM Band
Frequency Hopping Range:	iNET: Ten user-configurable 2.5 MHz-wide zones, each containing 8 frequencies (iNET) iNET-II: From one and up to 75 overlapping channels
Hop Patterns:	8192, based on network name
Frequency Stability:	20 ppm

TRANSMITTER:

Power Output (at antenna connector):	0.1 to 1.0 watt (+20 dBm to +30 dBm) ± 1.0 dB, <i>set by user</i>
Duty Cycle:	Continuous
Modulation Type:	Binary CPFSK
Output Impedance:	50 Ohms
Spurious:	–67 dBc
Occupied Bandwidth:	MDS iNET: 316.5 kHz MDS iNET-II: 600 kHz

RECEIVER:

Type:	Double conversion superheterodyne
Sensitivity:	MDS iNET: –92 dBm @ 512 kbps < 1×10^{-6} BER MDS iNET: –99 dBm @ 256 kbps < 1×10^{-6} BER MDS iNET-II: –92 dBm @ 1 Mbps < 1×10^{-6} BER MDS iNET-II: –97 dBm @ 512 kbps < 1×10^{-6} BER
Intermodulation:	59 dB Minimum (EIA)
Desensitization:	70 dB
Spurious:	60 dB

TRANSMIT/RECEIVE RANGE (Nominal)

	iNET-256 kbps	iNET-II-512 kbps
Fixed Range (typical):	15 miles (24 km)	12 miles (19 km)
Fixed Range (maximum):	60 miles (97 km)	30 miles (48 km)
Mobile Range (parked):	5 miles (8 km)	3 miles (5 km)
Mobile Range (moving):	3 miles (5 km)	1 mile (2 km)
:		
	iNET-512 kbps	iNET-II-1024 kbps
Fixed Range (typical):	8 miles (13 km)	8 miles (13 km)
Fixed Range (maximum):	15 miles (24 km)	15 miles (24 km)

Specifications subject to change without notice or obligation.

NOTE: Range calculations for fixed locations assume a 6 dBd gain Omnidirectional antenna on a 100 ft tower at the AP, a 10 dBd gain Yagi on a 25 ft mast at the remote with output power decreased to yield maximum allowable EIRP (36 dBm), a 10 dB fade margin, and a mix of agricultural and commercial terrain with line of sight.

Range calculations for mobile units assume a 6 dBd gain Omni on a 100 ft tower at the AP, a 5 dBd gain Omni with 1 watt output power at 6 ft height, a 10 dB fade margin, and 90% confidence with near line-of-sight in a mix of agricultural and commercial terrain.

Actual performance is dependent on many factors including antenna height, blocked paths, and terrain.

5.4 Channel Hop Table

The transceiver's hop table consists of 80 channels, numbered 0 to 79 as listed in Table 5-4. Center frequencies are calculated as follows (where F_n is the center frequency of channel n):

$$F_n = 902.5 \text{ MHz} + n \cdot 316.5 \text{ kHz}$$

The iNET-II transceiver operates on the same channel assignments, but because the modulation bandwidth is 600 kHz instead of 316.5 kHz it is recommended that the installer restrict channel usage to every other channel for units operating in the same area.

NOTE: Channels 24, 26, and 55 are not used.

Table 5-4. Channel Hop Table

Zone	Channel	Frequency
1	0	902.5000 (iNET FHSS lowest channel)
1	1	902.8165 (iNET-II DTS lowest channel)
1	2	903.1330
1	3	903.4495
1	4	903.7660
1	5	904.0825
1	6	904.3990
1	7	904.7155
2	8	905.0320
2	9	905.3485
2	10	905.6650
2	11	905.9815
2	12	906.2980
2	13	906.6145
2	14	906.9310
2	15	907.2475
3	16	907.5640
3	17	907.8805
3	18	908.1970
3	19	908.5135
3	20	908.8300
3	21	909.1465
3	22	909.4630
3	23	909.7795
4	24	910.0960
4	25	910.4125
4	26	910.7290
4	27	911.0455
4	28	911.3620
4	29	911.6785
4	30	911.9950
4	31	912.3115
5	32	912.6280
5	33	912.9445
5	34	913.2610
5	35	913.5775
5	36	913.8940
5	37	914.2105
5	38	914.5270
5	39	914.8435
6	40	915.1600

Table 5-4. Channel Hop Table (*Continued*)

Zone	Channel	Frequency
6	41	915.4765
6	42	915.7930
6	43	916.1095
6	44	916.4260
6	45	916.7425
6	46	917.0590
6	47	917.3755
7	48	917.6920
7	49	918.0085
7	50	918.3250
7	51	918.6415
7	52	918.9580
7	53	919.2745
7	54	919.5910
7	55	919.9075
8	56	920.2240
8	57	920.5405
8	58	920.8570
8	59	921.1735
8	60	921.4900
8	61	921.8065
8	62	922.1230
8	63	922.4395
9	64	922.7560
9	65	923.0725
9	66	923.3890
9	67	923.7055
9	68	924.0220
9	69	924.3385
9	70	924.6550
9	71	924.9715
10	72	925.2880
10	73	925.6045
10	74	925.9210
10	75	926.2375
10	76	926.5540
10	77	926.8705
10	78	927.1870 (iNET-II DTS highest channel)
10	79	927.5035 (iNET FHSS highest channel)

APPENDIX A. MDS INET/ENI PROTOCOLS

A.1 Introduction

This appendix covers the MDS iNET 900 ENI, which provides expanded gateway and protocol conversion capabilities not found in the MDS iNET 900. Throughout this document, the iNET 900 ENI is referred to as iNET/ENI. If iNET/ENI is required for your application, contact your factory representative to obtain the appropriate ENI file(s).

The iNET/ENI currently contains gateway conversion services for:

- **TCP, UDP, and PPP:** Identical to the iNET 900.
- **DF1 to EIP:** Provides EtherNet/IP (Ethernet Industrial Protocol) connectivity for DF1 full-duplex devices.
- **MODBUS to MODBUS TCP:** Provides Modbus TCP connectivity for Modbus RTU or Modbus ASCII Slave devices.

Additional gateway services and protocol support are planned for future firmware releases.

NOTE: This appendix assumes you have an understanding of Ethernet networking and TCP/IP.

A.2 Selecting New Protocols

Perform the following procedure to select one of the new protocols supported by the iNET/ENI:

1. Access the MDS iNET's Serial Configuration Wizard as described in this manual.
2. Select the IP Protocol screen displays. See Figure A-1 below.

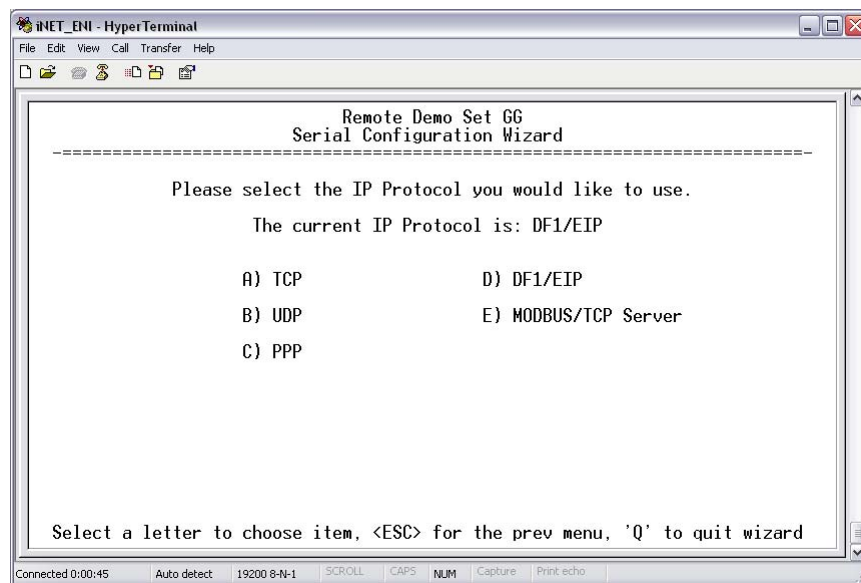


Figure A-1. Select IP Protocol Screen

3. Do one of the following:

- If you selected **D) DF1/EIP**, refer to *section A.3 on page 133* for information regarding DF1 to Ethernet/IP gateway services and configuration.
- If you selected **E) MODBUS/TCP Server**, refer to *Page 141* for information regarding MODBUS to MODBUS TCP gateway services and configuration.

A.3 DF1 to EIP Gateway Protocol

Introduction

The MDS iNET/ENI embeds the EtherNet/IP networking functionality of Rockwell's ENI adaptor into the iNET 900 transceiver. With some minor exceptions, the iNET/ENI duplicates the functionality of the 1761-NET-ENI, providing EtherNet/IP connectivity to any device using the full-duplex DF1 protocol (*Section* describes the differences between the iNET/ENI and the 1761-NET-ENI).

Why Use the iNET/ENI?

With the iNET/ENI, a separate EtherNet/IP adaptor is not needed when wireless EtherNet/IP networking is required for RS-232, full-duplex devices that use DF1 protocol, such as:

- MicroLogix™
- ControlLogix 1000 and 1500
- SLC 5/03, 5/05
- Other compatible DF1 devices and third-party products

The iNET/ENI also provides SMTP e-mail messaging from connected controllers to any destination on the network. See *Figure A-2*.

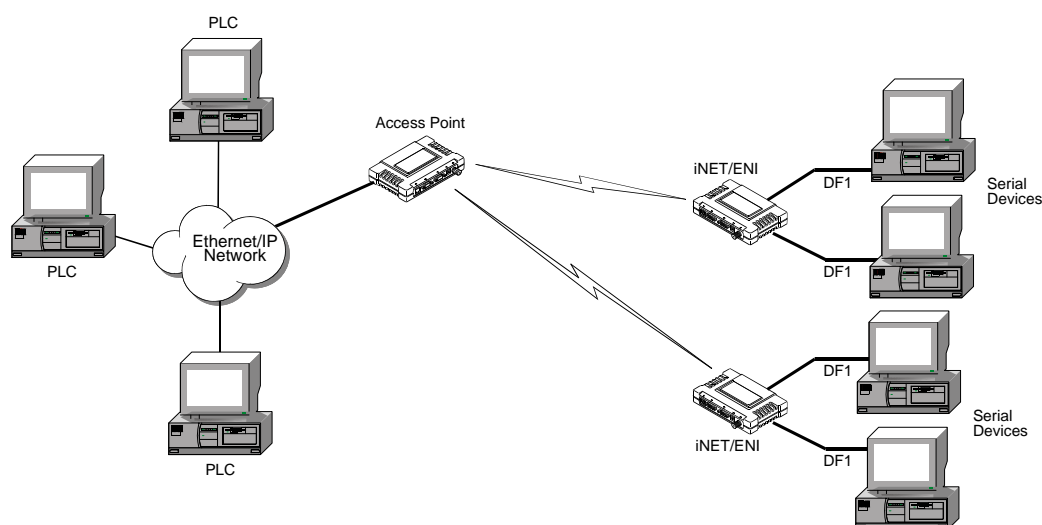


Figure A-2. Wireless Connectivity Using MDS iNET/ENI

Related Documentation

This supplement assumes you have an understanding of Ethernet/IP networking and the theory of operation for the 1761-NET-ENI adapter module. Refer to *Table A-1* for a list of documentation that can be downloaded from the Allen-Bradley web site: <http://www.ab.com/manuals>.

Table A-1. Related Documentation

For	Read this Document	Document No.
Instructions on Rockwell's ENI and ENIW adaptor.	MicroLogix™ Ethernet Interface User Manual	1761-UM006C-EN-P
Instructions on installing a 1761-NET-ENI or 1761-NET-ENIW Interface Converter.	Ethernet Interface Installation Instructions	1761-IN006
Information on DF1 open protocol.	DF1 Protocol and Command Set Reference Manual	1770-6.5.16
In-depth information on designing, implementing, and maintaining an industrial control system using EtherNet/IP.	EtherNet/IP Media Planning and Installation Manual	ENET-IN001
A glossary of industrial automation terms and abbreviations.	Allen-Bradley Industrial Automation Glossary	AG-7.1

Differences Between Allen-Bradley ENI and MDS iNET/ENI

The functional differences between the Allen-Bradley ENI and the MDS iNET/ENI include the following:

- The ENI allows up to two peers for outgoing messaging, two peers for incoming messaging, and two for messaging in either direction. The iNET/ENI is limited to 128 peers in any direction.
- The ENI supports configuration of the BOOTP Enable flag. The iNET/ENI supports configuration of DHCP Enable flags.
- The ENI supports saving configuration to both RAM and ROM. The iNET/ENI always stores configuration in ROM.
- The ENI uses CRC error checking for fixed baud rates and BCC/CRC auto-detect for autobaud. The iNET/ENI always uses BCC/CRC autodetect. This simplifies DF1 controller configuration while maintaining full backward compatibility.
- The ENI only has one serial port. The iNET/ENI has two serial ports, and supports both of them for data transfer. For the older ladder programs written for the ENI, the COM2 port is used as the default. To support setting a baud rate for the COM1 serial port, an additional configuration channel 247 is supported.
- The ENI does not support Ethernet message routing (that is, you cannot send a message from an Ethernet controller to the ENI and have it re-sent to another Ethernet controller). iNET/ENI supports Ethernet message routing to implement message transfer over the wireless link between several iNETs.

NOTE: Configuration of the iNET/ENI can be accomplished using the same two methods that function with Rockwell's ENI module:

1. With Rockwell ENI configuration utility connected to COM2 of the iNET/ENI.
2. Via EtherNet/IP using commands and structures listed for ENI in the 1761-NET-ENI User Manual.

In addition to these methods, configuration may also be performed using the standard user interface of the iNET transceiver and following through the Serial Port Configuration Wizard for DF1 to EtherNet/IP.

DF1/EIP PROTOCOL CONFIGURATION

NOTE: The Rockwell application will not identify the iNET/ENI radio properly unless the EDS file has been integrated the application using RSlinx software. If this has not already been done, refer to "EDS File Integration" on Page 145 for more information.

Perform the following procedure to configure the **DF1/EIP** IP protocol settings:

1. Press **A** if you want to change Security Descriptor Mask 1 from its default of **0.0.0.0**. In Figure A-3, Security Descriptor Mask 1 was changed to **192.158.16.255**. Press **B** if you want to change Security Descriptor Mask 2.
 2. Press **N** to continue.
Use the Security Descriptor Mask to control which IP addresses can access the serial device connected to the iNET/ENI. Values of 0 and 255 are considered "open," meaning any value in that position of the IP address is accepted. For example, the default value of **0.0.0.0** (or a value of **255.255.255.255**) would allow any IP address to access the device. In Figure A-3, only IP addresses beginning with 192.158.16 can access the device.
-

NOTE: The IP addresses shown in this manual are for example only. See your network administrator to determine the actual values you should use.

When using COM1, you must specify an expanded path to the target. To send a message to COM1, enter the following path: **<iNET/ENI IP Address>, 1, 1** where **1** is the COM1 output port and **1** is the destination address of the connected DF1 device.

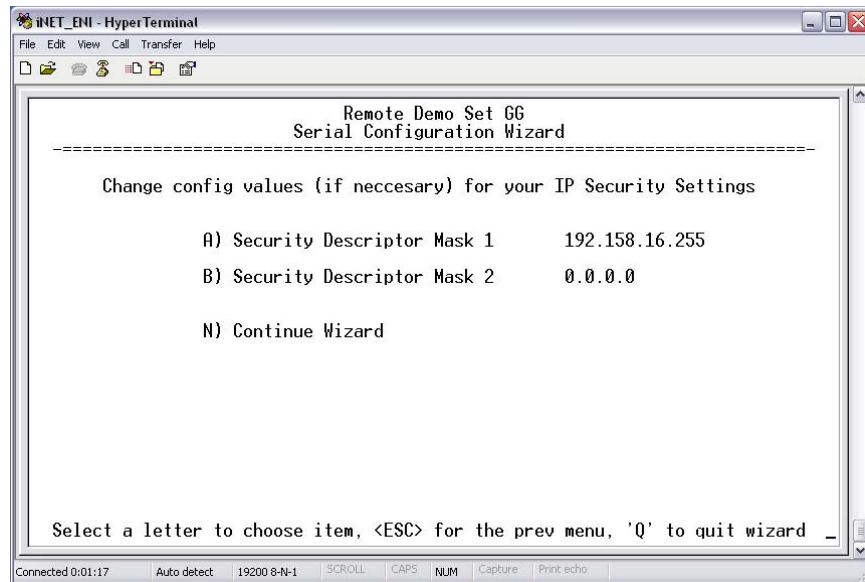


Figure A-3. Change Security Descriptor Mask

- Press **A** through **I** (and the **up/down arrow keys**, if necessary), then enter the appropriate IP addresses to configure the Message Routing table. See Figure A-4. When finished, press **N** to continue.

NOTE: The IP address fields shown in Figure A-4 are equivalent to the *Message Routing* table discussed in the Allen-Bradley MicroLogix™ Ethernet Interface User Manual (1761-UM006C-EN-P). Refer to that manual for more information.

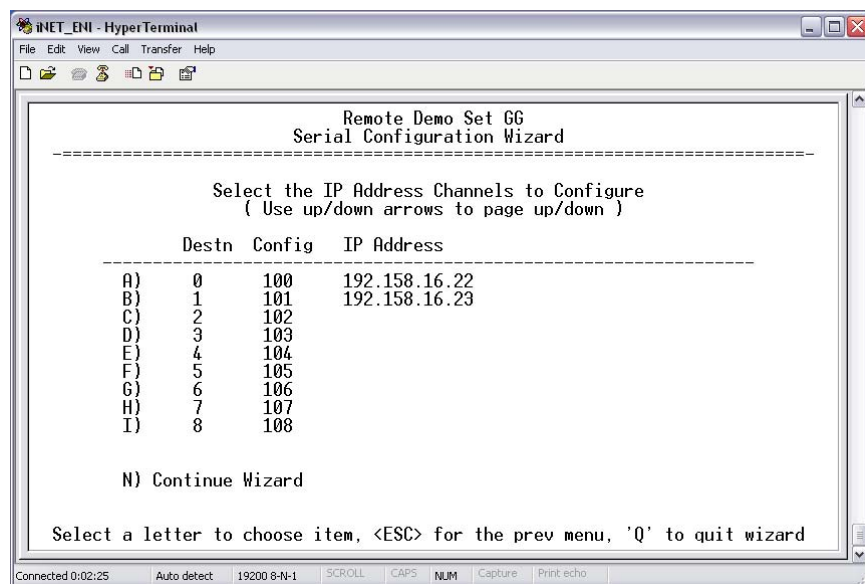


Figure A-4. Enter Destination IP Addresses

4. Press **A** to enter the IP address of the optional e-mail server, then press **B** to enter the **E-Mail From string** (the text that identifies who the sender was). See Figure A-5. When finished, press **N** to continue.

NOTE: The fields shown in Figure A-5 are equivalent to the *E-Mail Settings* table discussed in the *Allen-Bradley MicroLogix™ Ethernet Interface User Manual (1761-UM006C-EN-P)*. Refer to that manual for more information.

NOTE: E-Mail messages can only be sent from devices that generate string elements. The MicroLogix 1000 family of controllers *does not* generate string elements.

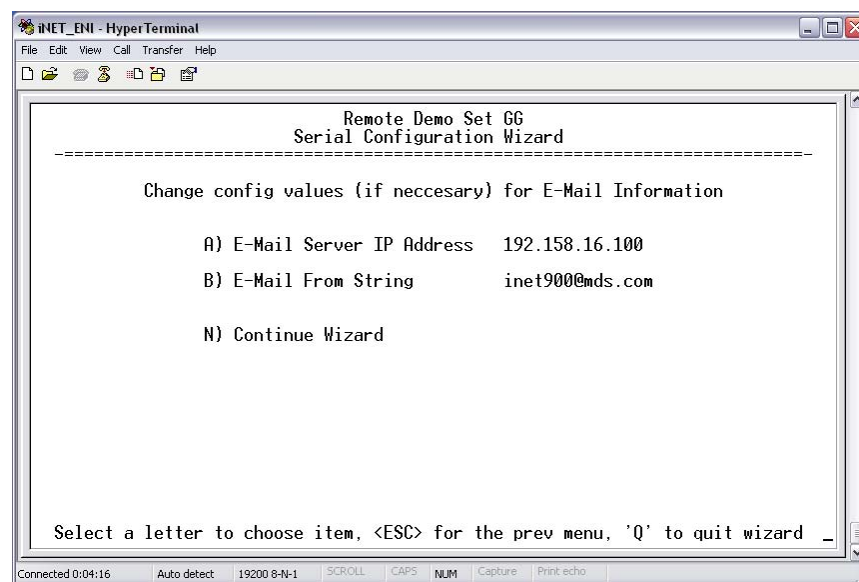


Figure A-5. Enter E-Mail Server IP Address and E-Mail From String

5. Press **A** through **I** (and the **up/down arrow keys**, if necessary), then enter the desired E-Mail Destination address(es) to configure the E-Mail Message Routing table. See Figure A-6. When finished, press **N** to continue.

NOTE: The fields shown in Figure A-6 are equivalent to the *E-Mail Routing* table discussed in the *Allen-Bradley MicroLogix™ Ethernet Interface User Manual (1761-UM006C-EN-P)*. Refer to that manual for more information.

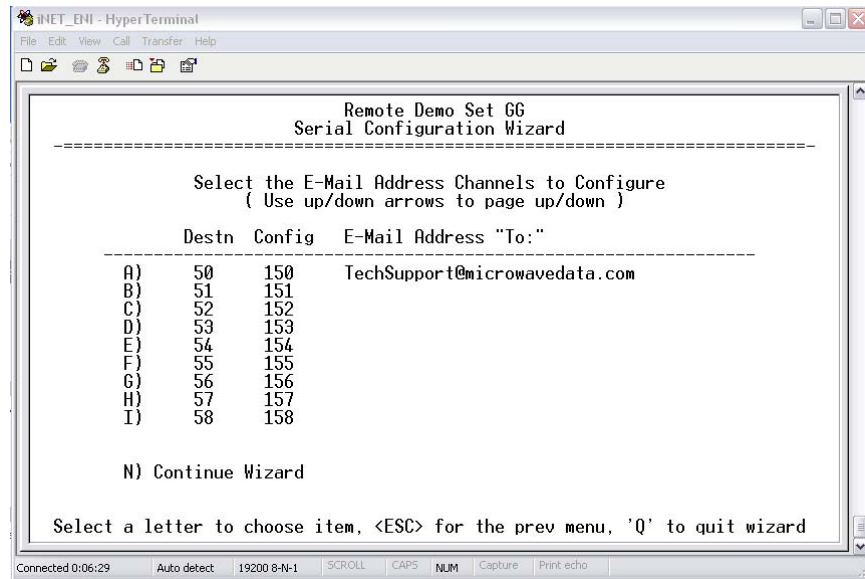


Figure A-6. Enter E-Mail Destination Addresses

6. Press **A** through **G** to select the baud rate you want the iNET/ENI to use when communicating with the serial device. See Figure A-7.

NOTE: The iNET/ENI defaults to Autobaud so that it automatically synchronizes with the connected device. The iNET/ENI, however, can only Autobaud to rates from 1200 to 38400. A baud rate of 57k must be configured manually.

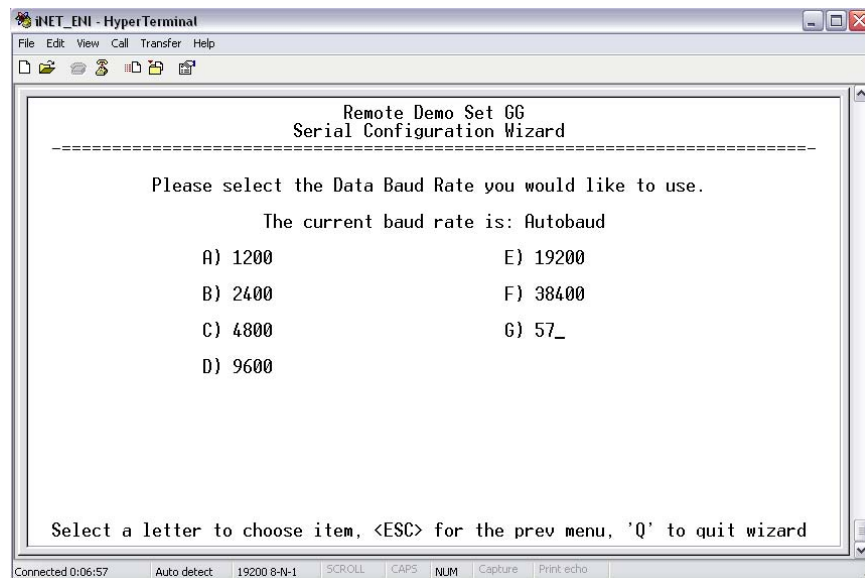


Figure A-7. Select Data Baud Rate

7. Press **A** to enable the iNET/ENI's COM2 port. See Figure A-8.

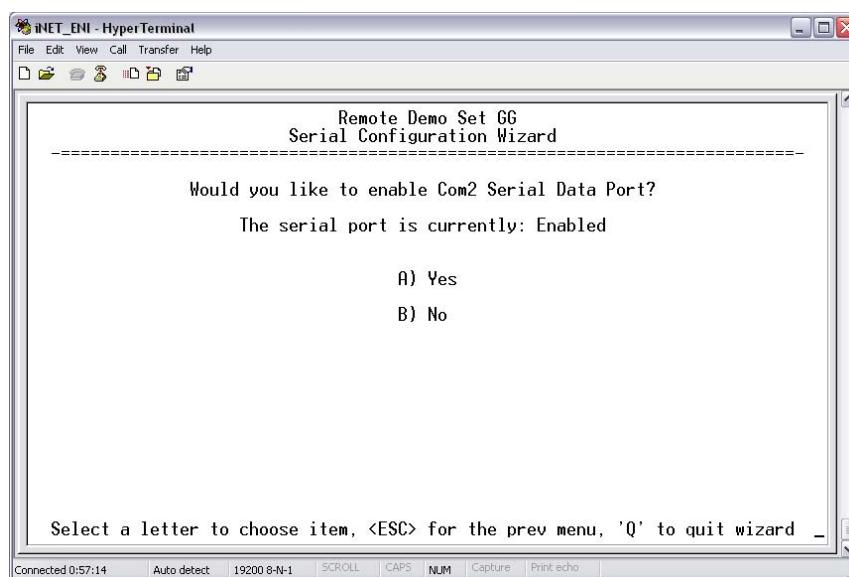


Figure A-8. Enable COM2 Data Port

8. Press **X** to save the COM2 port configuration changes. See Figure A-9.

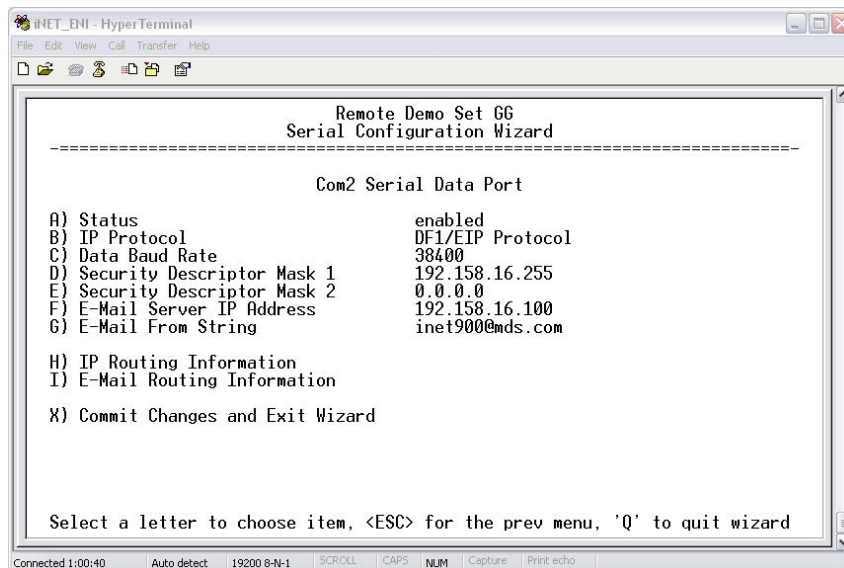


Figure A-9. Save COM2 Configuration Changes

9. The Wizard asks you to confirm that you want to save the changes. See Figure A-10. Press **Y** to save the changes and exit the Serial Configuration Wizard.

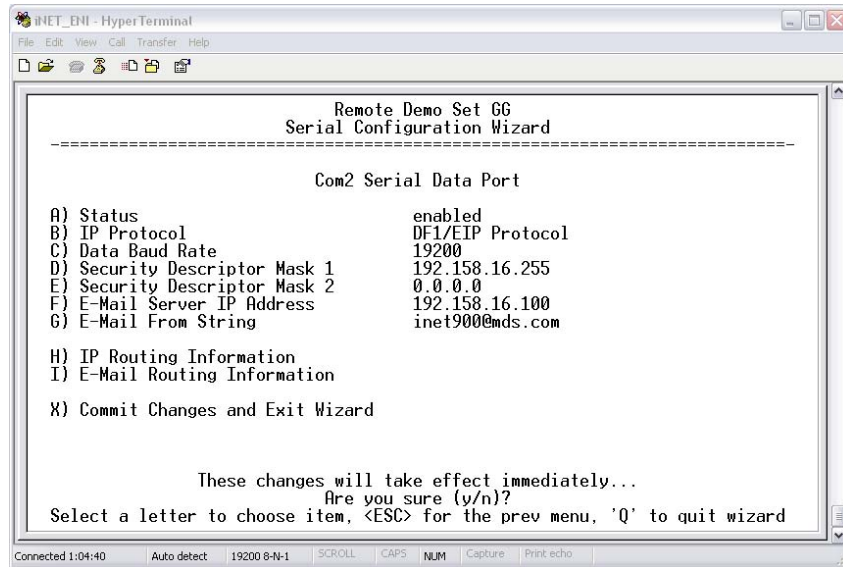


Figure A-10. Confirm Saving COM2 Changes

iNET/ENI Error Codes

Refer to Table A-2 for error codes generated by the iNET/ENI.

Table A-2. iNET/ENI Error Codes

Error Code	Description of Error Condition
10H	<p>Target node cannot respond because of incorrect command parameters or unsupported command. Possible causes:</p> <ul style="list-style-type: none"> • The message's data size is not valid • The data format is incorrect for any of the supported PCCC messages • Register parameters are not formatted correctly, or there is not enough data provided • RS-232 configuration packet data is not the correct size • The Node Address is invalid or out-of-range • The distant ENI/ENIW, controller, or device may not be responding • There may be a break in the connection between the ENI devices or controllers

Table A-2. iNET/ENI Error Codes (Continued)

Error Code	Description of Error Condition
30H	Target node responded with Remote station host is not there, disconnected, or shutdown.
D0H	Caused by one of the following: <ul style="list-style-type: none"> No IP address configured for the network or ENI not configured for Node Address used Bad command: unsolicited message error Bad address: unsolicited message error No privilege: unsolicited message error

A.4 MODBUS to MODBUS TCP Server Protocol

Introduction

NOTE: This section assumes you have an understanding of Ethernet networking, TCP/IP, and Modbus serial protocols. For more information, refer to the Modbus-IDA Organization web site: <http://www.modbus.org>.

The iNET implementation of the MODBUS to MODBUS TCP server protocol is limited to act as one of the following:

- A Modbus/TCP client on the LAN port
- A Modbus ASCII server on the serial port
- A Modbus RTU server (user configurable) on the serial port

NOTE: Modbus/TCP functionality is only available on the COM2 port of the iNET/ENI transceiver.

NOTE: All requests are sent using TCP on registered port 502.

NOTE: The PLC's User ID must match the last octet of the iNET Remote's IP address. See Figure A-11.

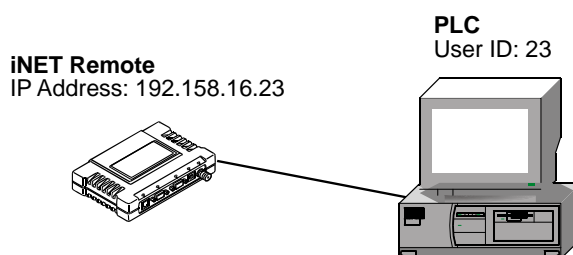


Figure A-11. PLC User ID Example

MODBUS/TCP Server Configuration

Perform the following procedure to configure the **MODBUS/TCP SERVER** IP protocol settings:

1. Press **A** to select the listening port for the MODBUS/TCP server. See Figure A-12. The default is port **502**. Then press **N** to continue.

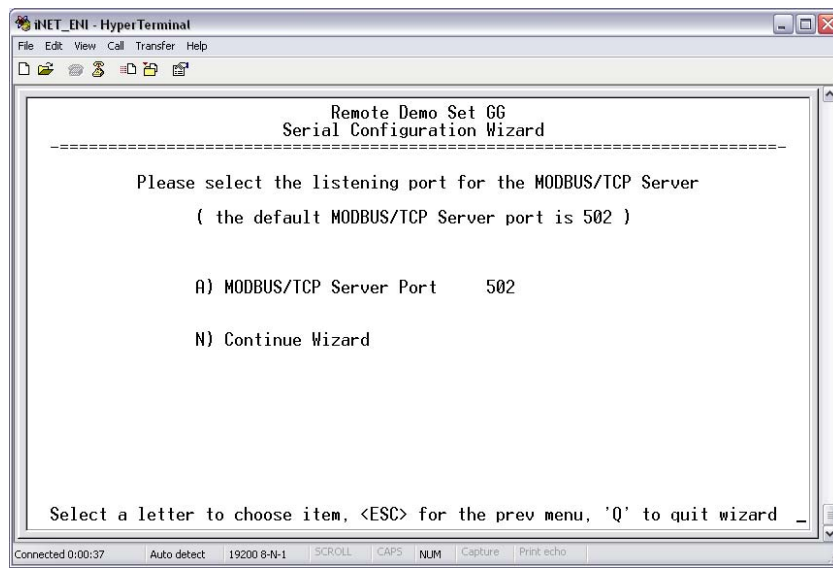


Figure A-12. MODBUS/TCP Server Listening Port

2. Press **A** to change the MODBUS serial format, then press the **space bar** to toggle between the available formats (**MODBUS/RTU** or **MODBUS/ASCII**). Press **B** to enter the MODBUS serial timeout value. See Figure A-13. Press **N** to continue.

NOTE: The only difference between MODBUS/RTU and MODBUS/ASCII is the form of the framing sequence, error check pattern, and address interpretation.

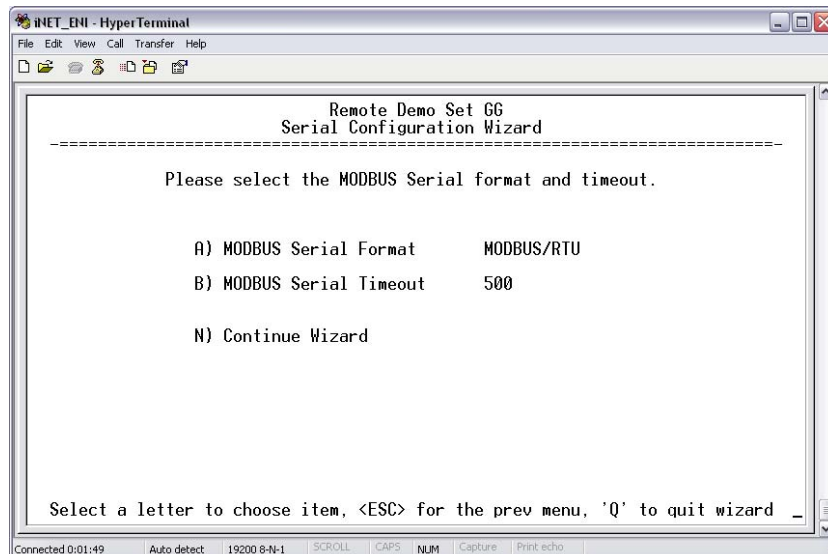


Figure A-13. Choose MODBUS Serial Format and Timeout

3. Press **A** through **H** to select the desired data baud rate. See Figure A-14.

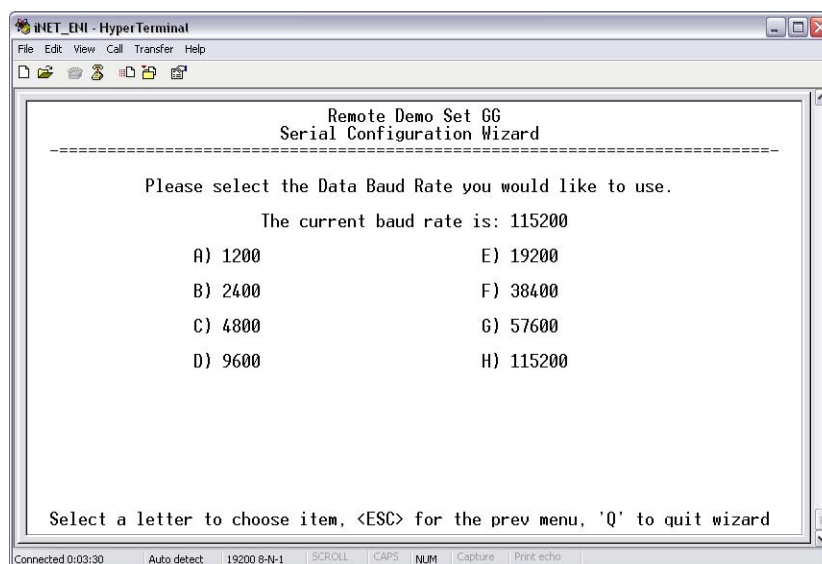


Figure A-14. Select Data Baud Rate

4. Press **A** through **L** to select the desired byte format. See Figure A-15.

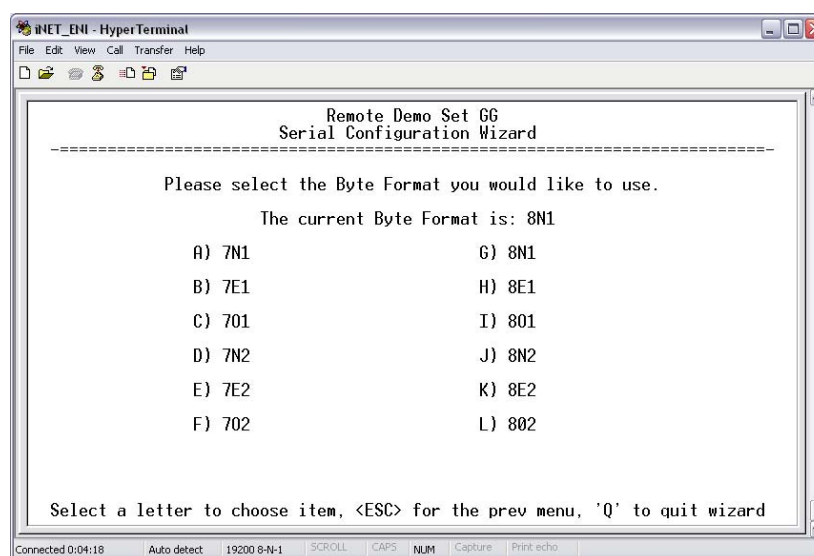


Figure A-15. Select Byte Format

5. Press **A** to enable hardware flow control. Press **B** to disable hardware flow control. See Figure A-16.

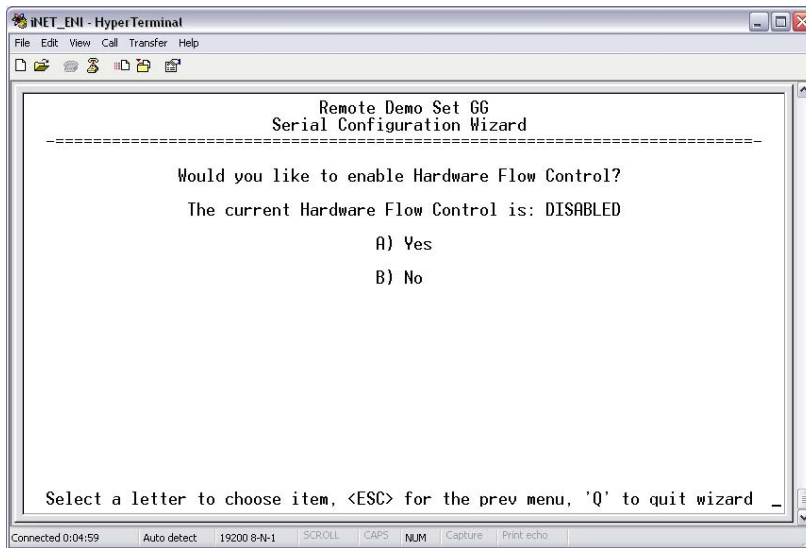


Figure A-16. Enable/Disable Hardware Flow Control

6. Press **A** to enable the iNET/ENI's COM2 port. See Figure A-17.

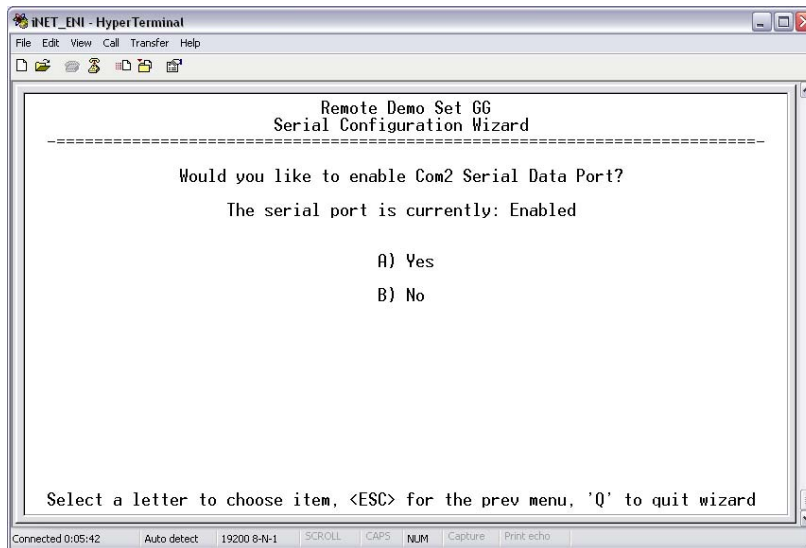


Figure A-17. Enable COM2 Data Port

7. Press **X** to save the COM2 port configuration changes. See Figure A-18.

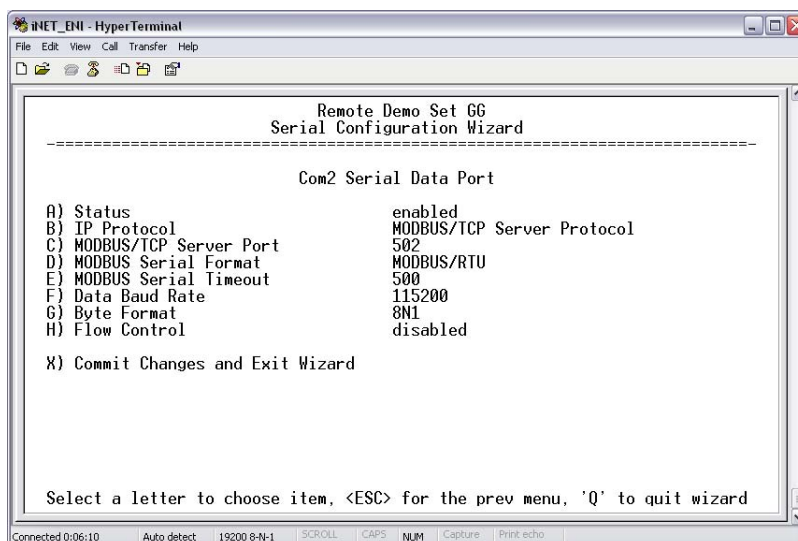


Figure A-18. Save COM2 Configuration Changes

8. The Wizard asks you to confirm that you want to save the changes. See Figure A-19. Press **Y** to save the changes and exit the Serial Configuration Wizard.

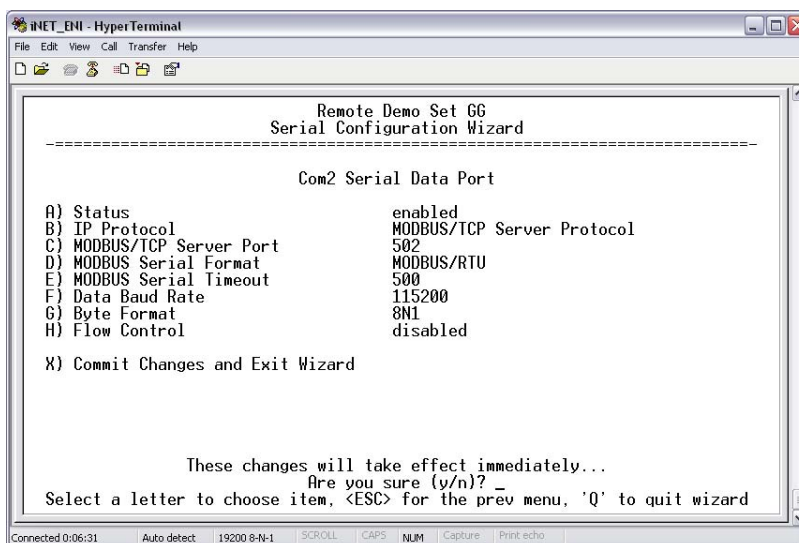


Figure A-19. Confirm Saving COM2 Changes

EDS File Integration

The Electronic Data Sheet (EDS) file must be integrated into the Rockwell Software RSlinx application for the MDS iNET icon to be properly displayed. The RSlinx software includes an EDS Wizard to make this process a straightforward task. Follow the prompts and dialog boxes in the wizard to complete the integration process.

Figure A-20 shows the first screen in the EDS Wizard.

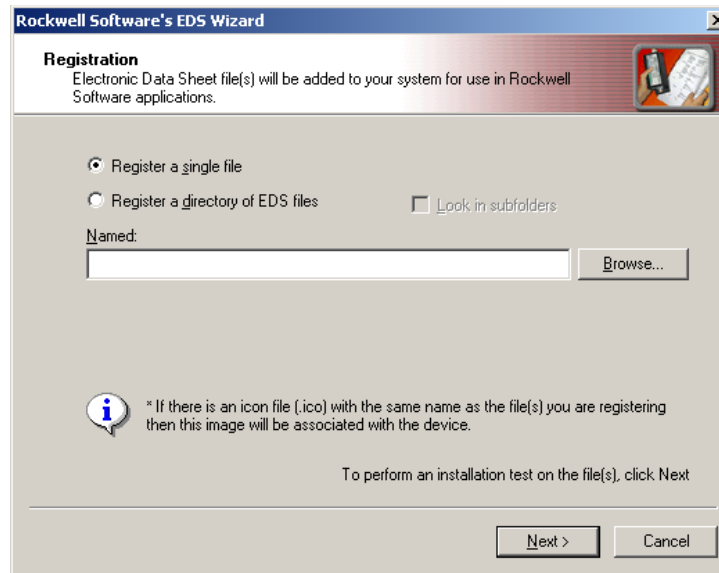


Figure A-20. Rockwell Software's EDS Wizard
(Appears after selecting "Add" from the Hardware Installation Tool)

Pressing "Next," brings up a series of screens where you select the EDS file to download, and specify the registration options.

Figure A-21 shows the MDS iNET icon about to be integrated into the RSlinx software. The default iNET icon is displayed, but it may be changed to another representation of the radio, if desired, by selecting "Change icon" and choosing another image.

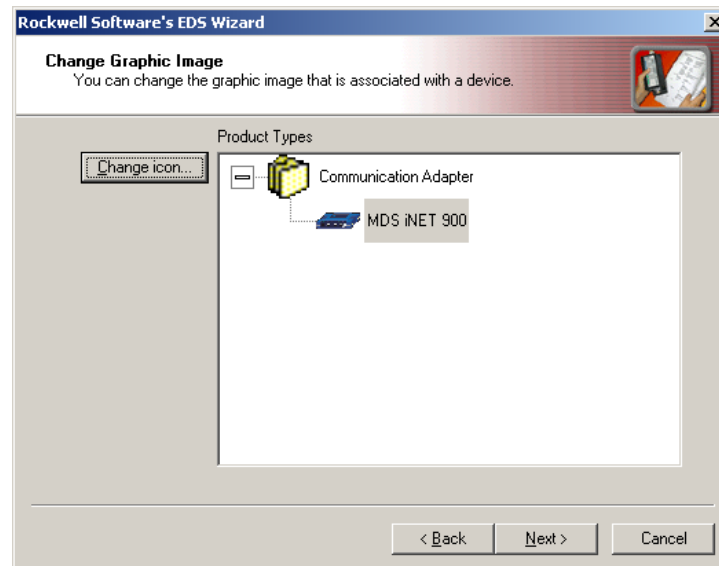


Figure A-21. Graphic Image Screen
(Default iNET icon shown)

Select "Next" to go to the Final Task Summary screen where the MDS iNET icon can be registered. After successful registration, a Completion screen appears (Figure A-22), indicating that the wizard has been completed. From here, you select "Finish" to return to the Hardware Installation Tool.



Figure A-22. EDS Wizard Completion Screen

APPENDIX B. GLOSSARY OF TERMS & ABBREVIATIONS

If you are new to wireless IP/Ethernet systems, some of the terms used in this guide may be unfamiliar. The following glossary explains many of these terms and will prove helpful in understanding the operation of your radio network.

Access Point (AP)—The transceiver in the network that provides synchronization information to one or more associated Remote units. AP units may be configured for either the Access Point (master) or Remote services. (See “Network Configuration Menu” on Page 27.)

Active Scanning—See *Passive Scanning*

Antenna System Gain—A figure, normally expressed in dB, representing the power increase resulting from the use of a gain-type antenna. System losses (from the feedline and coaxial connectors, for example) are subtracted from this figure to calculate the total antenna system gain.

AP—See *Access Point*

Association—Condition in which the frequency hopping pattern of the Remote is synchronized with the Access Point station and is ready to pass traffic.

Authorization Key—Alphanumeric string (code) that is used to enable additional capabilities in the transceiver.

Bit—The smallest unit of digital data, often represented by a one or a zero. Eight bits (plus start, stop, and parity bits) usually comprise a byte.

Bits-per-second—See *BPS*.

BPDU—Bridge Protocol Data Units

BPS—Bits-per-second (bps). A measure of the information transfer rate of digital data across a communication channel.

Byte—A string of digital data usually made up of eight data bits and start, stop and parity bits.

CSMA/CA—Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD—Carrier Sense Multiple Access/Collision Detection

Cyclic Redundancy Check (CRC)—A technique used to verify data integrity. It is based on an algorithm which generates a value derived from the number and order of bits in a data string. This value is compared with a locally-generated value and a match indicates that the message is unchanged, and therefore valid.

Datagram—A data string consisting of an IP header and the IP message within.

dB_i—Decibels referenced to an “ideal” isotropic radiator in free space. Frequently used to express antenna gain.

dB_m—Decibels referenced to one milliwatt. An absolute unit used to measure signal power, as in transmitter power output, or received signal strength.

DCE—Data Circuit-terminating Equipment (or Data Communications Equipment). In data communications terminology, this is the “modem” side of a computer-to-modem connection. COM1 Port of the transceiver is set as DCE.

Decibel (dB)—A measure of the ratio between two signal levels. Frequently used to express the gain (or loss) of a system.

Delimiter—A flag that marks the beginning and end of a data packet.

DHCP (Dynamic Host Configuration Protocol)—An Internet standard that allows a client (i.e. any computer or network device) to obtain an IP address from a server on the network. This allows network administrators to avoid the tedious process of manually configuring and managing IP addresses for a large number of users and devices. When a network device powers on, if it is configured to use DHCP, it will contact a DHCP server on the network and request an IP address.

The DHCP server will provide an address from a pool of addresses allocated by the network administrator. The network device may use this address on a “time lease” basis or indefinitely depending on the policy set by the network administrator. The DHCP server can restrict allocation of IP addresses based on security policies. An Access Point may be configured by the system administrator to act as a DHCP server if one is not available on the wired network.

DTE—Data Terminal Equipment. A device that provides data in the form of digital signals at its output. Connects to the DCE device.

DTS—Digital Transmission System

Encapsulation—Process in by which, a complete data packet, such as Modbus frame or any other polled asynchronous protocol frame, is placed in the data portion of another protocol frame (in this case IP) to be transported over a network. Typically this action is done at the receiving end, before being sent as an IP packet to a network. A similar reversed process is applied at the other end of the network extracting the data from the IP envelope, resulting in the original packet in the original protocol.

Endpoint—IP address of data equipment connected to the ports of the radio.

Equalization—The process of reducing the effects of amplitude, frequency or phase distortion with compensating networks.

Fade Margin—The greatest tolerable reduction in average received signal strength that will be anticipated under most conditions. Provides an allowance for reduced signal strength due to multipath, slight antenna movement or changing atmospheric losses. A fade margin of 15 to 20 dB is usually sufficient in most systems.

Fragmentation—A technique used for breaking a large message down into smaller parts so it can be accommodated by a less capable media.

Frame—A segment of data that adheres to a specific data protocol and contains definite start and end points. It provides a method of synchronizing transmissions.

Frequency Hopping—The spread spectrum technique used by the transceiver, where two or more associated radios change their operating frequencies several times per second using a set pattern. Since the pattern appears to jump around, it is said to “hop” from one frequency to another.

Frequency Hopping Spread Spectrum (FHSS)—See Frequency Hopping.

Frequency Zone—The radio uses up to 80 discrete channels in the 902 to 928 MHz spectrum. A group of 8 channels is referred to as a zone; in total there are 10 zones.

Hardware Flow Control—A transceiver feature used to prevent data buffer overruns when handling high-speed data from the connected data communications device. When the buffer approaches overflow, the radio drops the clear-to-send (CTS) line, that instructs the connected device to delay further transmission until CTS again returns to the high state.

Hop Pattern Seed—A user-selectable value to be added to the hop pattern formula in an unlikely event of nearly identical hop patterns of two collocated or nearby radio networks to eliminate adjacent-network interference.

Host Computer—The computer installed at the master station site, that controls the collection of data from one or more remote sites.

HTTP—Hypertext Transfer Protocol

IAPP (inter-Access Point Protocol)—A protocol by which access points share information about the stations that are connected to them. When a station connects to an access point, the access point updates its database. When a station leaves one access point and roams to another access point, the new access point tells the old access point, using IAPP, that the station has left and is now located on the new access point.

ICMP—Internet Control Message Protocol

IGMP (Internet Gateway Management Protocol)—Ethernet level protocol used by routers and similar devices to manage the distribution of multicast addresses in a network.

IEEE—Institute of Electrical and Electronic Engineers

Image (File)—Data file that contains the operating system and other essential resources for the basic operation of the radio's CPU.

LAN—Local Area Network

Latency—The delay (usually expressed in milliseconds) between when data is applied at the transmit port at one radio, until it appears at the receive port at the other radio.

MAC—Media Access Control

Management Systems—User interface used to manage the unit.

MD5—A highly secure data encoding scheme. MD5 is a one-way hash algorithm that takes any length of data and produces a 128 bit “fingerprint.” This fingerprint is “non-reversible,” it is computationally infeasible to determine the file based on the fingerprint. For more details review “RFC 1321” available on the Internet.

MIB—Management Information Base

Microcontroller Unit—See *MCU*.

Mobile IP—An emerging standard by which access points and stations maintain network connectivity as the stations move between various IP networks. Through the use of Mobile IP a station can move from its home IP network to a foreign network while still sending and receiving data using its original IP address. Other hosts on the network will not need to know that the station is no longer in its home network and can continue to send data to the IP address that was assigned to the station. Mobile IP also uses DHCP when the station moves into a foreign network.

Mobile Station—Refers to a station that moves about while maintaining active connections with the network. Mobility generally implies physical motion. The movement of the station is not limited to a specific network and IP subnet. In order for a station to be mobile it must establish and tear down connections with various access points as it moves through the access points' territory. To do this, the station employs roaming and Mobile IP.

MS—See Management Systems.

MTBF—Mean-Time Between Failures

Multiple Address System (MAS)—See *Point-Multipoint System*.

Network Name—User-selectable alphanumeric string that is used to identify a group of radio units that form a communications network. The Access Point and all Remotes within a given system should have the same network address.

Network-Wide Diagnostics—An advanced method of controlling and interrogating GE MDS radios in a radio network.

NTP—Network Time Protocol

Packet—The basic unit of data carried on a link layer. On an IP network, this refers to an entire IP datagram or a fragment thereof.

Passive Scanning—Scanning is a process used by stations to detect other access points on network to which it may connect if it needs to roam. Passive scanning is a slower process in which it listens for information offered by the access points on a regular basis. Active scanning is a faster process in which the station sends out probe message to which the access points respond. Passive scanning can be done while maintaining the current network connectivity. Active scanning affects the RF configuration of the radio and therefore, at least temporarily, disconnects the station from the access point.

PING—Packet Internet Groper. Diagnostic message generally used to test reachability of a network device, either over a wired or wireless network.

Point-Multipoint System—A radio communications network or system designed with a central control station that exchanges data with a number of remote locations equipped with terminal equipment.

Poll—A request for data issued from the host computer (or master PLC) to a remote radio.

Portability—A station is considered connected when it has successfully authenticated and associated with an access point. A station is considered authenticated when it has agreed with the access point on the type of encryption that will be used for data packets traveling between them. The process of association causes a station to be bound to an access point and allows it to receive and transmit packets to and from the access point. In order for a station to be associated it must first authenticate with the access point. The authentication and association processes occur automatically without user intervention.

Portability refers to the ability of a station to connect to an access point from multiple locations without the need to reconfigure the network settings. For example, a remote transceiver that is connected to an access point may be turned off, moved to new site, turned back on, and, assuming the right information is entered, can immediately reconnect to the access point without user intervention.

PLC—Programmable Logic Controller. A dedicated microprocessor configured for a specific application with discrete inputs and outputs. It can serve as a host or as an RTU.

PuTTY—A free implementation of Telnet and SSH for Win32 and Unix platforms. It is written and maintained primarily by Simon Tatham. Refer to <http://www.pobox.com/~anakin/> for more information.

Remote—A transceiver in a network that communicates with an associated Access Point.

RFI—Radio Frequency Interference

Roaming—A station's ability to automatically switch its wireless connection between various access points (APs) as the need arises. A station may roam from one AP to another because the signal strength or quality of the current AP has degraded below what another AP can provide. When two access points are co-located for redundancy, roaming allows the stations to switch between them to provide a robust network. Roaming may also be employed in conjunction with Portability where the station has been moved beyond the range of the original AP to which it was connected. As the station comes in range of a new AP, it will switch its connection to the stronger signal. Roaming refers to a station's logical, not necessarily physical, move between access points within a specific network and IP subnet.

RSSI—Received Signal Strength Indicator

RTU—Remote Terminal Unit. A data collection device installed at a remote radio site.

SCADA—Supervisory Control And Data Acquisition. An overall term for the functions commonly provided through an MAS radio system.

SNMP—Simple Network Management Protocol

SNR—Signal-to-Noise Ratio. A measurement of the desired signal to ambient noise levels. This measurement provides a relative indication of signal quality. Because this is a relative number, higher signal-to-noise ratios indicate improved performance.

SNTP—Simple Network Time Protocol

SSL—Secure Socket Layer

SSH—Secure Shell

STP—Spanning Tree Protocol

SWR—Standing-Wave Ratio. A parameter related to the ratio between forward transmitter power and the reflected power from the antenna system. As a general guideline, reflected power should not exceed 10% of the forward power ($\approx 2:1$ SWR).

TCP—Transmission Control Protocol

TFTP—Trivial File Transfer Protocol

Trap Manager—Software that collects SNMP traps for display or logging of events.

UDP—User Datagram Protocol

UTP—Unshielded Twisted Pair

WINS—Windows Internet Naming Service. Part of Microsoft Windows NT and 2000 servers that manages the association of workstation names and locations with Internet Protocol addresses. It works without the user or an administrator having to be involved in each configuration change. Similar to DNS.

Zone—See *Frequency Zone*.

NOTES

NOTES

[illegible]

Index

Numerics

100BaseT 106
10BaseT 106
802.11b 7

A

Access Point (AP), defined 148
Active Scanning, defined 148, 151
Actual Data Rate 70
Add Associated Remotes 66
AgeTime 79
alarm conditions 99
 correcting 100
Alarmed 97
Antenna
 aiming 115
 directional 112
 omnidirectional 110
 polarization 110
 selection 109
 SWR check 114
 system gain 148
 system gain, defined 148
 Yagi 110
AP
 Auto Upgrade 77
 Reboot when Upgraded 77
application
 IP-to-Serial 57
 Mixed-Modes 63
 Point-to-Multipoint Serial-to-Serial 59
 Point-to-Point Serial-to-Serial 61
Approved
 Access Points/Remotes List 66
 Remotes/Access Points List 66
Associated 97
Association
 Date 77
 defined 148
 Process 76
 Time 77
Auth Traps Status 37
Authorization Key 89
 defined 148
Authorized Features 89
Auto Data Rate Menu
 SNR Threshold/Delta 46
Auto Key Rotation 65, 66
Auto-Upgrade/Remote-Reboot 90

B

Backhaul
 for Serial Radio Networks 5
 Network 6
bandpass filter 112
Beacon
 Period 41, 118, 119
 signal 76
Begin Wizard 52
Bit, defined 148
Bits-per-second (bps), defined 148
BPDU 118

 defined 148
BPS, defined 148
bridging 128
 remote-to-remote 29
Bytes
 defined 148
 in on port 81
 in on socket 82
 out on port 82
 out on socket 82
 received 74
 sent 74

C

cable
 feedlines 110
Clear
 Com# statistics 82
 Ethernet stats 74
 Log 72
 Wireless stats 74
Client Inactivity Timeout 55
Collocating Multiple Radio Networks 10
Commit Changes and Exit Wizard 53, 54, 55, 56, 57
compression 41, 118
configuration 53, 54
 basic device parameters 25
 DHCP server 35
 editing files 88
 Ethernet Port 33
 file 94
 PPP Mode 56
 radio parameters 40
 scripts 87
 SNMP Agent 36
 TCP Mode 54
 UDP mode 52
Connection Status 77
connectors 124
Contact 26
cost of deployment 6
Count 92, 93
CRC (Cyclic Redundancy Check), defined 148
CSMA
 CA, defined 148
 CD, defined 148
Current
 Alarms 72
 AP IP Address 77
 AP Mac Address 77
Custom Data Buffer Size 53, 54, 55, 56, 57

D

data
 baud 56
 baud rate 53, 54, 55, 56
 buffering 51, 55
 compression 118
 rate 41
Datagram, defined 148
DataRate 79
Date 26
 Format 26
dB, defined 148
dBi, defined 148
dBm

- defined 148
- watts-volts conversion 117
- DCE, defined 148
- defaults
 - reset to factory 92
- Delete
 - All Remotes 66
 - Remote 66
- Delimiter, defined 148
- deployment costs 6
- Description 26
- Device
 - IP Address 56
 - Mode 22
 - Name 22, 26, 27
 - Status 23, 97
- DHCP
 - defined 149
 - Netmask 35
- Diagnostic Tools 98
- dimensions 107
- DKEY command 114
- DNS Address 35
- DTE 7, 49
- Dwell Time 41, 119

E

- EIA-232 7
- Encapsulation, defined 149
- Encryption 66
 - Phrase 66
- Ending Address 35
- Endpoint
 - defined 149
 - Listing 70
 - Listing Menu 79
- ENI, MDS iNET 900 1
- Equalization, defined 149
- Ethernet
 - Link (H/W) Watch 34
 - Link Poll Address 34
 - Packet Statistics 74
 - port enabled/disabled 34
 - Rate Limit 34, 35
- Event Log 70, 71, 97, 99, 100, 102

F

- Fade Margin 149
- Feedline
 - selection 109, 110
- Filename 72, 83
- firewall 120
- firmware
 - installing 84
 - upgrade 84, 90
 - version 23, 25
- Flow Control 51, 53, 54, 55, 56
 - hardware, defined 149
- Force Key Rotation 66
- Force Reboot 90
- Fragmentation
 - defined 149
 - Threshold 41, 119
- Frame, defined 149
- Frequency 91
 - zone, defined 149

- fuse replacement 126

G

- gain
 - antenna, defined 148
 - system 113
- Glossary 148-152
- Go 92

H

- Hardware
 - flow control, defined 149
 - Version 23, 25
- Hop
 - Format 42
 - pattern 112
 - Pattern Seed 41
 - Sync 97
- Hopping
 - channels 129
- HTTP
 - defined 149
 - Security Mode 65

I

- IETF standard RFC1213 36
- IGMP 50
 - defined 150
- Image
 - Copy 83
 - file, defined 150
 - Verify 83
- iNET II, differences of 1, 40, 41, 46, 48, 80, 109, 111, 115
- Installation
 - antenna & feedline 109
 - feedline selection 110
 - general information 1
 - requirements 106
 - site selection 108
 - site survey 112
- Interference 112
- Internet
 - Assigned Numbers Authority 50
- IP 35
 - Addr 92
 - Address 23, 78, 79, 88
 - Gateway 88
 - Mobile, defined 150
 - Protocol 52, 54, 55, 56
 - tunneling 49

K

- Key
 - transmitter, for antenna SWR check 114
- KEY command 114

L

- LAN
 - defined 150
- Latency 118
- Latency, defined 150
- Latest AP Firmware Version 77
- LED
 - LAN 95
 - LINK 95, 112, 115

- PWR 71, 73, 95, 99, 102
 - use during troubleshooting 95
- Link Established 57
- Local
 - Area Network, defined 150
 - IP Port 53, 54
 - Listening IP Port 56
- Location 26, 88
- Logged Events 102
- Lost Carrier Detected 74, 98

M

- MAC Address 78, 79, 118
- Management System
 - user interfaces 16
- MD5, defined 150
- MDS iNET 900 ENI 1
- MDS Security Suite 11
- measurements
 - radio 114
- MIB
 - defined 150
 - files 36
- Mobile IP, defined 150
- Mobility 47
- Mobility Capability 8
- MODBUS 55
- Mode
 - serial gateway interface 8
 - TCP 8
 - UDP 8
- Model Number 25
- MTBF, defined 150
- Multicast
 - IP Address 52
 - IP Port 53
- multiple
 - protocols 6
 - services 6

N

- NEMA 7
- Network
 - Name 10, 22
 - Name, defined 150
 - Time Protocol (NTP), defined 150
- network design 8
 - antennas 9
 - collocating multiple radio networks 10
 - network name 9
 - repeaters 8
 - using multiple Access Points 9
 - Using the AP as a Store-and-Forward Packet Repeater 9
 - using two transceivers to form a repeater station 8
- NTP (Network Time Protocol), defined 150

O

- Owner 26

P

- Packet
 - defined 150
 - Redundancy Mode 53, 54
 - Size 92, 93
 - Statistics 70, 74, 98

- Packets
 - Dropped 74, 98
 - Packets-per-Second 118
 - Received 74
 - Received by Zone 75
 - Sent 74
- Passive Scanning, defined 151
- Performance Information Menu 119
- PING 112
 - defined 151
- Ping Utility 92
- PLC 7
 - defined 151
- Point-Multipoint System, defined 151
- Point-to-Point
 - LAN Extension 5
 - Link 5
- Poll, defined 151
- port
 - antenna 115
 - COM1 7, 49, 59, 109, 125
 - COM2 7, 49, 59, 125
 - IP 59
 - LAN 124
 - not Enabled 57
 - well-known 120
- Portability, defined 151
- ports
 - serial 6
- power
 - how much can be used 112
 - transmitter power output 114
- PPP 50
- Primary Host Address 55
- Primary IP Port 55
- Programmable Logic Controller 7
- protocol
 - BPDU 118
 - IP 35, 49
 - MODBUS 55
 - PPP 50
 - SNMP 14, 36, 120
 - defined 151
 - SNTP 151
 - STP 118
 - STP, defined 152
 - TCP 49, 54, 58, 62, 118
 - defined 152
 - TFTP 84
 - defined 152
 - UDP 49, 50, 58, 61, 62, 118
- PuTTY usage 18
 - defined 151

R

- Radio
 - Frequency Interference 10, 112
 - Remote, defined 151
 - Test 90
- range, transmission 7
- Read Community String 36
- Reboot
 - Device 84
 - on Upgrade 90
- Receive errors 74, 98

- Received Signal Strength Indicator 109
 - defined 151
- Redundancy
 - Using multiple Access Points 9
- Remote
 - IP Address 54
 - IP Port 54
 - Listing 70
 - Listing Menu 78
 - Performance Listing 70, 80
 - radio, defined 151
 - Terminal Unit 7
 - Terminal Unit, defined 151
- Repeater 8
 - antennas 9
 - Network Name 9
 - Using the AP as a Store-and-Forward Packet Repeater 9
 - Using two transceivers to form a repeater station 8
- reprogramming 83
- Restart DHCP Server 36
- Retries 74, 98
- Retrieve File 83, 88
- Retry errors 74, 98
- RetryEr 80
- RF Output Power 40, 70
- RFI 10
 - defined 151
- Roaming, defined 151
- RSSI 91, 98, 109, 115
 - by Zone 70, 71
 - defined 151
 - Threshold 42
- RTS Threshold 41, 119
- RTS/CTS handshaking 53
- RTU 7, 49, 59, 62
 - defined 151
- RxBCCMC 80
- RxPkts 79, 80
- RxRate 80
- RxViaEP 80
- S**
- Save Changes 66
- SCADA 6, 7, 50
 - defined 151
- Scanning 97
 - Active, defined 151
 - Passive, defined 151
- Seamless Inter-Frame Delay 53, 54, 55, 56, 57
- Secondary
 - Host Address 55
 - IP Port 55
- security
 - Approved Access Points/Remotes List 66
 - Auto Key Rotation 65, 66
 - encryption 66
 - Encryption Phrase 66
 - Force Key Rotation 66
 - general information 2
 - HTTP Security Mode 65
 - suite 11
 - Telnet Access 65
 - Two-Way Authentication 65
 - User Password 65
- Send
 - File 88
 - Log 72
- Sending LCP Requests 57
- Serial
 - Configuration Wizard 51
 - Data Statistics 81
 - encapsulation 49
 - Mode 53, 54, 55, 56, 57
 - Number 23, 25
 - Port Statistics 98
 - radio networks, backhaul 5
- Server Status 35
- Signal strength 109
- Signal-to-Noise Ratio 70
 - defined 151
- Simple Network
 - Management Protocol, defined 151
 - Time Protocol, defined 151
- Site selection 108
- SNMP 14
 - defined 151
 - Mode 37, 65
 - usage 120
 - V3 Passwords 37
- SNR 42
 - defined 151
 - Threshold 42
- SNTP
 - defined 151
- Spanning Tree Protocol 118
- Spanning Tree Protocol, defined 152
- Specifications 126–129
- SSH, defined 152
- SSL, defined 151
- Standing Wave Ratio 152
- Starting
 - Address 35
 - Information Screen 25
- State 79
- Status 23, 52, 54, 55, 56
- STP, defined 152
- Support Bundle
 - file 92
- SWR 114, 152
 - performance optimization 114
- Syslog Server 72
- system gain, antenna 148
- system gain, antenna (defined) 148
- T**
- TCP 8, 62, 118
 - Client 49
 - defined 152
 - Server 49
- Telnet 59
 - Access 65
- Test Mode 91
- TFTP
 - defined 152
 - Host Address 72, 83, 88
 - Time-out 72
 - Timeout 83, 88
- Time 26
- Time to Live (TTL) 53
- Transmission
 - Control Protocol, defined 152
 - range 7

transparent encapsulation 49

Trap

- Community String 37

- Manager 37

- Manager, defined 152

- Version 37

Troubleshooting 94–105

- Using the Embedded Management System 95

Two-Way Authentication 65

TX Output Power 91

TxKey 91

TxPkt 79

TxPkts 80

TxViaEP 80

U

UDP 8, 50, 61, 62, 118

- defined 152

- mode 52

Unit Name 88

Uptime 23, 25

User Password 65

Using multiple Access Points 9

V

V3

- Authentication Password 37

- Privacy Password 37

via Remote 79

View

- Approved Remotes 66

- Current Alarms 73

- Current Settings 52

- Event Log 73

- Log 72

VLAN 28, 29, 30, 64

- Configuring for operation with 30

- Configuring IP Address with VLAN disabled 32

- Configuring IP Address with VLAN enabled 31

volts-dBm-watts conversion 117

W

watts-dBm-volts conversion 117

WINS

- Address 35

- defined 152

Wireless

- Network Status 70, 76

- Packet Statistics 74

wizard

- serial configuration 51

Write community String 36

Y

Yagi antenna 110

Z

Zone, defined 152

IN CASE OF DIFFICULTY...

GE MDS products are designed for long life and trouble-free operation. However, this equipment, as with all electronic equipment, may have an occasional component failure. The following information will assist you in the event that servicing becomes necessary.

TECHNICAL ASSISTANCE

Technical assistance for GE MDS products is available from our Technical Support Department during business hours (8:00 A.M.–5:30 P.M. Eastern Time). When calling, please give the complete model number of the unit, along with a description of the trouble/symptom(s) that you are experiencing. In many cases, problems can be resolved over the telephone, without the need for returning the unit to the factory. Please use one of the following means for product assistance:

Phone: 585 241-5510 E-Mail: gemds.techsupport@ge.com
FAX: 585 242-8369 Web: www.gemds.com

FACTORY SERVICE

Component level repair of this equipment is not recommended in the field. Many components are installed using surface mount technology, which requires specialized training and equipment for proper servicing. For this reason, the equipment should be returned to the factory for any PC board repairs. The factory is best equipped to diagnose, repair and align your unit to its proper operating specifications.

If return of the equipment is necessary, you will be issued a Service Request Order (SRO) number. The SRO number will help expedite the repair so that the equipment can be repaired and returned to you as quickly as possible. Please be sure to include the SRO number on the outside of the shipping box, and on any correspondence relating to the repair. No equipment will be accepted for repair without an SRO number.

A statement should accompany the unit describing, in detail, the trouble symptom(s), and a description of any associated equipment normally connected to the product. It is also important to include the name and telephone number of a person in your organization who can be contacted if additional information is required.

The unit must be properly packed for return to the factory. The original shipping container and packaging materials should be used whenever possible. All factory returns should be addressed to:

GE MDS
Product Services Department
(SRO No. XXXX)
175 Science Parkway
Rochester, NY 14620 USA

When repairs have been completed, the equipment will be returned to you by the same shipping method used to send it to the factory. Please specify if you wish to make different shipping arrangements. To inquire about an in-process repair, you may contact our Product Services Group at 585-241-5540 (FAX: 585-242-8400), or via e-mail at productservices@gemds.com.



Digital Energy
MDS

GE MDS, LLC
175 Science Parkway
Rochester, NY 14620
General Business: +1 585 242-9600
FAX: +1 585 242-9620
Web: www.gemds.com

